



Security Research

PASR

Preparatory Action on the enhancement of the European industrial potential in the field of Security research



Grant Agreement no. 108600
Supporting activity acronym: PRISE

Activity full name:
Privacy enhancing shaping of security research and technology – A participatory approach to
develop acceptable and accepted principles for European Security Industries and Policies

Activity type: Supporting Activity

Annex to D 5.4 German Report Interview meeting about security technology and privacy

Start date of Activity: 1 February 2006

Duration: 28 month

Author(s):
Maren Raguse, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Revision 1

Supporting Activity Co-ordinator Johann Čas,
Institute of Technology Assessment, Austrian
Academy of Sciences
Strohgassee 45, A-1030 Vienna, Austria
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Partners **Institute of Technology Assessment,**
Vienna, Austria
Contact: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita



The Danish Board of Technology,
Copenhagen, Denmark
Contact: Lars Klüver
LK@Tekno.dk
www.tekno.dk

TEKNOLOGI-RÅDET

The Norwegian Board of Technology,
Oslo, Norway
Contact: Christine Hafskjold
christine.hafskjold@teknologiradet.no
www.teknologiradet.no



**Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein,**
Kiel, Germany
Contact: Marit Hansen
LD10@datenschutzzentrum.de
www.datenschutzzentrum.de



Legal notice:

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of the following information.

Table of Contents	page
Annex 1 - Participants background	5
Annex 2 - Program of the interview meeting	7
Annex 3 - Material sent to the participants	9
Annex 4 - Questionnaire	30
Annex 5 - Transcript of group interviews	60
Annex 6 - Frequency tables	115
Annex 7 - Comments from the questionnaire	205

Annex 1 - Participants background

The 31 registered citizens span the following diversification on the selection matrix described in the interview-meeting manual (D 1.3):

age	18-34			35-54			55+			
education	low	medium	high	low	medium	high	low	medium	high	Σ
female		2	2	2		1		2	4	13
male		6			4	4	1	1	2	18
Σ	0	8	2	2	4	5	1	3	6	31

Table 1: matrix of registered participants

The following matrix describes the diversification of participants who showed up on the day of the meeting:

age	18-34			35-54			55+			
education	low	medium	high	low	medium	high	low	medium	high	Σ
female		1	1		1	1		3	1	8
male		3	1		1	3		2	3	13
Σ	0	4	2	0	2	4	0	5	4	21

Table 2: matrix of actual participants

When translating the interview questionnaire prior to the interview meeting, fitting the German educational system's stages and degrees¹ into the provided scheme turned out to be difficult. Furthermore, a deviation occurred, as in two boxes of the matrix the final number of participants fulfilling the applicable criteria exceeded the number of registered participants with that same criteria (table 2 – marked red). The reason for this discrepancy lies in the level of detail for the educational background description. While in the registration form the participants were asked to fill in their 'educational background', the actual questionnaire listed a choice between specifically defined options (possible answers to question no. 6):

¹ For a detailed description see Eurybase – The Information Database on Education Systems in Europe: The Education System in Germany 2004/2005. Available at http://www.eurydice.org/ressources/Eurydice/pdf/eurybase/2006_DNDE_EN.pdf and an overview given by the German ministry of Education and Research: http://www.bmbf.de/pub/bildung_in_deutschland.pdf (p. 5).

No.	English template for translation	Austrian translation of questionnaire	German translation of questionnaire
1.	Elementary School – 7 years of schooling	Volks- oder Hauptschule	Volks- oder Hauptschulabschluss
2.	Intermediate School – 8 or 9 years of schooling	Lehre	Realschulabschluss
3.	Vocational training (skilled level / craftsman's training)	Allgemeinbildende oder berufsbildende höhere Schule	Fachabitur
4.	Secondary school (high-school graduation)	Kolleg	Abitur
5.	Short-term higher education (less than 3 years of study)	Bakkalaureat	Lehre oder Ausbildung
6.	Medium length higher education (3 - 4 years of study)	Fachhochschule oder Universität	Fachhochschule oder Universität
7.	Advanced higher education (more than 4 years of study)		

Key: **Low education** **Medium education** **High education**

Table 3: Mapping of possible answers to question 6 to selection matrix

Most participants, when filling in the form in the registration letter, listed their current profession instead of the level of education received. Many professions in Germany can be achieved with different levels of education. For this reason an exact mapping of the registered citizens to the matrix prior to the interview-meeting was impossible.

Annex 2 - Program of the interview meeting

ULD • Postfach 71 16 • 24171 Kiel

«Geschlecht» «Vorname» «Nachname»
«Adresse»

«PLZ» «Ort»

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
Frau Raguse
Durchwahl: 988-1284
Aktenzeichen:
LD10.4-64.12/01.034

Kiel, 25. Mai 2007

Ihre Anmeldung zu der Befragung am 15.06.2007 im Rahmen eines EU-Forschungsprojektes

«Anrede» «Nachname»,

vielen Dank für Ihre Anmeldung zu einem Interview-Treffen über Privatsphäre und Sicherheitstechnologien. Wir haben aus den Anmeldungen Sie als Teilnehmer ausgewählt.

**Wir freuen uns, Sie am
Freitag den 15. Juni um 16.00 Uhr
in der IHK zu Kiel - Bergstraße 2, 24103 Kiel -
begrüßen zu dürfen.**

Wir sind auf Ihre Meinung und Sichtweise über Privatsphäre und Sicherheitstechnologien gespannt. Zur Vorbereitung auf das Treffen senden wir Ihnen mit diesem Schreiben einige Szenarien, die zur Einstimmung auf das Thema dienen sollen. Zusätzlich möchten wir gerne während des Treffens Ihre Diskussionsbeiträge auf Tonband aufzeichnen. Die Beiträge werden nach der Diskussion pseudonymisiert abgeschrieben und die Tonaufzeichnungen vernichtet. Weitere Hinweise zu diesem Punkt entnehmen Sie bitte der Anlage.

Das Interview-Treffen

Die Methode des Interview-Treffens wurde entwickelt, um die Meinung von Bürgern zu komplexen Sachverhalten zu erfahren und zwar insbesondere zu Fragen, bei denen der Einzelne oft über wenige Vorkenntnisse verfügt. Das Hauptziel des Treffens besteht darin, ein umfangreiches Verständnis der bestehenden Meinungen und Argumente zu gewinnen. Dies bedeutet auch, dass es keine ‚richtigen‘ oder ‚falschen‘ Antworten geben wird auf die zu diskutierenden Fragen. Ganz im Gegenteil zeichnet sich ein erfolgreiches Interview-Treffen dadurch aus, dass es auf eine ungezwungene, lebhafte und respektvolle Art und Weise durchgeführt wird, bei der jeder Teilnehmer die Gelegenheit erhält, seine Standpunkte zu vertreten.

Nachdem Sie sich einen Platz gesucht haben und sich einander vorgestellt haben, strukturiert sich das Treffen in drei Abschnitte.

Zunächst wird ein Experte zu Fragen des Datenschutzes und Sicherheitstechnologien das Thema vorstellen. Damit soll jedem Teilnehmer ein gemeinsamer Eindruck entstehen, welche zentralen Probleme es in diesem Zusammenhang gibt. Sie werden die Möglichkeit haben, Fragen zu stellen.

- 2 -

Danach werden wir Sie bitten, einen Fragebogen zu Ihrer Meinung und Einstellung im Bezug auf neue Sicherheitstechnologien und deren Einsatz in unterschiedlichen Situationen auszufüllen. Wir sind dabei jederzeit bereit, Ihnen bei Fragen zum Ablauf zu helfen.

Schließlich werden die Teilnehmer in kleinere Gruppen von 6-9 Personen aufgeteilt, um tiefergehend die angeregten Fragestellungen zu diskutieren. Diese Gruppendiskussionen werden von geschulten Mitarbeitern moderiert.

Abschließend werden sich alle Teilnehmer noch einmal zusammen finden und es gibt die Möglichkeit für abschließende Fragen und Anmerkungen.

Zeitlicher Ablauf:

16:00 – 16:15 Begrüßung
16:15 – 16:50 Einführung durch Experten und Fragen
16:50 – 17:40 Ausfüllen des Fragebogens
17:40 – 17:50 Einteilung in Gruppen
17:50 – 18:50 Gruppendiskussion
18:50 – 19:00 Zusammenkommen und abschließende Bemerkungen

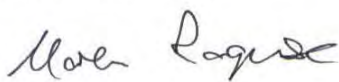
Erfrischungen werden während der ganzen Dauer des Treffens zur Verfügung stehen.

Vorbereitung:

Beigefügt finden Sie einige Szenarien über Sicherheitstechnologien und Datenschutzfragen. Diese Szenarios stellen mögliche Entwicklungen im Bereich der Sicherheitstechnologien und unterschiedliche Umgangsweisen mit diesen Entwicklungen. Sie sind in der Form von Alltagserfahrungen von zwei Personen abgefasst und sollen einen einfachen Bezug ermöglichen. Zusätzlich enthalten Sie einige Fakten über Sicherheitstechnologien. Wir möchten Sie bitten, diese Szenarien zu lesen und auf sich wirken zu lassen als Vorbereitung auf das Treffen. Viele der aufgeworfenen Fragen stehen im Bezug zu den dargestellten Problemfeldern.

Für weitere Fragen stehen wir gerne zur Verfügung.

Mit freundlichen Grüßen



Maren Raguse

Unabhängiges Landeszentrum für Datenschutz
Projektleitung PRISE
Telefon: 0431 – 988 1284, Email: LD104@datenschutzzentrum.de

Annex 3 - Material sent to the participants

- Flyer put up at vocational school: page 10
- newspaper advertisement: page 11
- invitation letter: page 12 - 15
- project description German (annex to invitation letter): page 16
- information concerning tape recording: page 17
- scenarios: page 18 - 29



EU-Forschungsprojekt sucht

Teilnehmer

an einer **Befragung** zum Spannungsfeld

**Innere Sicherheit und Sicherheitstechnologien
vs.
Privatsphäre und Datenschutz**

Dauer der Befragung: ca. 3h
Termin: Freitag **15.6.2007**
Zeit: 16h bis 19h

Durchgeführt wird das Treffen mit ca. 30 Teilnehmern vom Unabhängigen Landeszentrum für Datenschutz im Rahmen des EU-Forschungsprojekts PRISE.

Für Ihre Teilnahme erhalten Sie von uns als Dankeschön eine Aufmerksamkeit und können zudem EU-Sicherheitsforschung mitgestalten.

**Für mehr Informationen und Anmeldung:
www.datenschutzzentrum.de/prise/umfrage**

Projektleiterin Maren Raguse
Telefon: 0431 – 988 1284
E-Mail: LD104@datenschutzzentrum.de





ULD • Postfach 71 16 • 24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
Maren Raguse
Durchwahl: 988-1284
Aktenzeichen:
LD10.4-64.12/01.034

Kiel, 3. Mai 2007

Sehr geehrte Damen und Herren,

Ihre Meinung ist gefragt

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) lädt Sie ein, Ihre Ansichten und Meinung über Privatsphäre und Sicherheitstechnologien in einem Interview-Treffen zu vertreten.

Freitag, den 15. Juni 2007 von 16:00 bis ca. 19:00 Uhr

Das Treffen findet in Kiel statt. Den genauen Ort erhalten Sie mit Ihrer Anmeldebestätigung.

Warum Privatsphäre und Sicherheitstechnologien?

Man mag sich dessen oft nicht bewusst sein, aber es werden immer mehr Informationen über unsere Aktivitäten in unterschiedlichen Situationen gesammelt und gespeichert: beispielsweise wenn man eine E-Mail versendet oder empfängt, wenn man von einer Kamera am Bahnhof gefilmt wird oder wenn man etwa mit einer EC- oder Kreditkarte bezahlt. Dies ist eine Folge von fortgeschrittenen Sicherheitstechnologien. Diese Technologien können unser Sicherheitsgefühl erhöhen, indem sie zur Verhütung oder Aufklärung von Verbrechen oder Terrorismus beitragen und sie können auch unser tägliches Leben bequemer gestalten.

Diese Entwicklungen bei Sicherheitstechnologien können aber auch problematisch sein. Wie können wir ein Gleichgewicht finden zwischen einem sicheren und bequemen täglichen Leben einerseits und der Gefahr von Verletzungen der Privatsphäre, ungerechtfertigten Beschuldigungen und dem Missbrauch persönlicher Daten andererseits? Dies ist das Dilemma, das wir gerne mit Ihnen diskutieren würden.

- 2 -

Warum gerade ich?

Entwicklungen bei Sicherheitstechnologien werden Einfluss auf jeden von uns haben. Es ist daher wichtig, die Standpunkte jener Personen zu berücksichtigen, die in Zukunft mit diesen Technologien leben werden - Sie gehören dazu! Sie sind eine von vielen, zufällig aus dem Telefonbuch ausgewählten Personen in Kiel und Umgebung, die diesen Brief erhalten. Eine zufällige Auswahl hilft uns, mit Personen mit unterschiedlichen Erfahrungen und Meinungen in Kontakt zu treten. Dies bedeutet auch, dass wir keinerlei Vorkenntnisse über Sicherheitstechnologien von Ihnen erwarten, sondern nur den Wunsch, unsere gemeinsame Zukunft mit zu gestalten.

Was ist ein Interview-Treffen?

Das Treffen ist ein zwangloses Zusammenkommen nach der Arbeit und wird etwa drei Stunden dauern. Sie werden etwa 30 weiteren Teilnehmerinnen und Teilnehmern mit unterschiedlichem Hintergrund begegnen; keiner von ihnen wird besondere Kenntnisse im Bereich Sicherheitstechnologien besitzen. Ein Experte wird das Spannungsfeld zwischen Privatsphäre und Sicherheitstechnologien vorstellen und es wird die Möglichkeit geben, Fragen zu stellen. Im Anschluss werden Sie gebeten, einen Fragebogen auszufüllen. Abschließend werden Szenarien zu zukünftigen Sicherheitstechnologien unter Anleitung geschulter Mitarbeiter in kleineren Gruppen diskutiert.

Die Teilnahme ist kostenlos und wir werden eventuelle Fahrtkosten (mit öffentlichen Verkehrsmitteln) erstatten. Während des Treffens werden wir Erfrischungen für Sie bereithalten. Als Zeichen der Anerkennung werden Sie zudem eine kleine Aufmerksamkeit erhalten.

Während des Treffens möchten wir Ihre Diskussionsbeiträge auf Tonband aufzeichnen; alle Ihre Beiträge werden nach dem Treffen anonymisiert werden.

Was ist der Anlass?

Das Interview-Treffen ist ein wichtiger Teil des EU-Projekts PRISE. Dieses Forschungsprojekt wird von vier Institutionen in Österreich, Dänemark, Deutschland und Norwegen durchgeführt. All diese Einrichtungen haben große Erfahrung in der Einschätzung und Bewertung neuer Technologien. Die Interview-Treffen werden in Österreich, Dänemark, Deutschland, Norwegen, Spanien und Ungarn durchgeführt.

Das Ergebnis des PRISE-Projekts werden Empfehlungen für die zukünftige Entwicklung von Sicherheitstechnologien in der Europäischen Union sein. Die bei den Treffen vertretenen Standpunkte werden ein wesentliches Element im Projekt darstellen.

Mehr Informationen über PRISE können Sie der beigefügten Kurzbeschreibung entnehmen. Sie können auch die Projekthomepage unter <http://prise.ocaw.ac.at> besuchen (diese Informationen sind allerdings nur in Englisch vorhanden).

- 3 -

Wie kann ich teilnehmen?

Melden Sie sich bitte online an über das Webformular unter www.datenschutzzentrum.de/prise/ oder nutzen Sie das beigelegte Formular; wir bitten um Ihre Antwort bis zum 14. Mai.

Falls sich mehr als 30 Personen anmelden, werden wir eine Auswahl treffen, um eine möglichst gemischte Gruppe zu erhalten. Alle angemeldeten Personen werden eine Antwort vor dem 26. Mai erhalten. Diejenigen, die ausgewählt werden, erhalten einen detaillierten Plan für das Interview-Treffen sowie eine kurze Einführung zu wichtigen neuen Sicherheitstechnologien.

Falls Sie nicht teilnehmen wollen, brauchen Sie gar nichts zu tun. Wir werden weder Ihren Namen noch Ihre Adresse speichern.

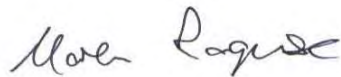
Kontakt

Falls Sie irgendwelche Fragen oder Anmerkungen haben, wenden Sie sich bitte an:

Unabhängiges Landeszentrum für Datenschutz
Maren Raguse
Holstenstraße 98
24103 Kiel
Telefon: 0431 – 988 1284
LD104@datenschutzzentrum.de

Wir freuen uns auf Ihre Antwort!

Mit freundlichen Grüßen



Maren Raguse
Unabhängiges Landeszentrum für Datenschutz
Projektleitung PRISE



- 4 -

Bitte melden Sie sich für das PRISE Interview-Treffen am 15.06.2007
von 16:00 bis 19:00 Uhr an:

- per Internet unter: www.datenschutzzentrum.de/prise/
oder
- per Telefon unter 0431 - 988 1284
oder
- per Fax 0431 – 988 1223 mit diesem Formular
oder
- per unfreiem Antwortbrief mit diesem Formular an die Adresse:
ULD – Projekt PRISE
Holstenstr. 98
24103 Kiel

Bitte melden Sie sich bis zum 14. Mai 2007 bei uns an. Nach der Anmeldung bekommen
Sie weitere Informationen.

Bitte füllen Sie alle Pflichtfelder aus (gekennzeichnet durch*)

*Name:

*Adresse:

*Ort:

*Postleitzahl:

*Telefon:

*E-Mail:

*Geschlecht:

*Alter:

*Ausbildung:

Gründe für die Teilnahme (freiwillige Angabe):

.....
.....
.....



PRISE Grundrechte und Bürgerakzeptanz für Sicherheitsforschung und -anwendungen

Ziel

Das Projekt **PRISE** soll zu einer sicheren Zukunft der Europäischen Union im Einklang mit den Grundrechten, insbesondere dem Schutz der Privatsphäre, und den Wünschen der europäischen Bürgerinnen und Bürger beitragen.

Motivation

Die Europäische Union wird im Rahmen ihres 7. Forschungsrahmenprogramms erhebliche Geldmittel für die Erforschung und Entwicklung von Technik und Anwendungen aufwenden, die der inneren Sicherheit dienen. Damit diese neue Technik nicht die Grundrechte und insbesondere den Schutz der Privatsphäre gefährdet, sondern ein Maß zwischen Sicherheit und persönlicher Freiheit findet, das den Wünschen der europäischen Bürgerinnen und Bürger entspricht, erarbeitet **PRISE** als vorbereitende Aktivität im Rahmen des PASR-Programms der Europäischen Union Richtlinien und Kriterien für die Sicherheitsforschung und die Anwendung der entwickelten Sicherheitslösungen. Das Projekt wird so die Europäische Union bei der Gestaltung zukünftiger Programme zur Sicherheitsforschung im Sinne ihrer eigenen Grundwerte unterstützen.

Aufgaben

- Entwicklung von Kriterien und Richtlinien zur grundrechtskonformen Sicherheitsforschung und Technikentwicklung
- Umsetzung der Ergebnisse in Szenarien, die die Kriterien zur grundrechtskonformen Gestaltung von Sicherheitstechnologien in unterschiedlichem Ausmaß berücksichtigen
- Überprüfen dieser Szenarien in partizipativen Technikfolgen-Abschätzungs-Verfahren in unterschiedlichen europäischen Staaten, um zu einer Einschätzung der Wünsche der Bürgerinnen und Bürger zu gelangen
- Weiterentwicklung der Kriterien und Richtlinien unter Einbeziehung von Anbietern von Sicherheitstechnik, privaten und öffentlichen Anwendern, Gestaltern der Sicherheitspolitik und von Organisationen, die zur Sicherheitspolitik möglicherweise in Konflikt stehende Interessen vertreten
- Verbreitung der Ergebnisse bei den für die Gestaltung von Sicherheitstechnik und -anwendungen verantwortlichen Akteuren.

Ergebnisse

Die in **PRISE** erarbeiteten Kriterien und Leitlinien für die Sicherheitsforschung und daraus resultierende Anwendungen sollen die europäische Sicherheitsindustrie und deren Kunden in die Lage versetzen, Produkte und Dienstleistungen im Einklang mit den Grundwerten der Europäischen Union und den Wünschen ihrer Bürgerinnen und Bürger zu entwickeln und einzusetzen. Dies erhöht die Akzeptanz von Sicherheitsmaßnahmen in der Bevölkerung und damit die Glaubwürdigkeit der Europäischen Union als Wertegemeinschaft. Es fördert überdies die Wettbewerbsfähigkeit der europäischen Sicherheitsindustrie, indem diese darin unterstützt wird, einerseits für den europäischen Markt besonders geeignete Produkte und Dienstleistungen zu entwickeln und andererseits Grundrechtskonformität und Bürgerakzeptanz als Wettbewerbsvorteil international zu vermarkten.

PRISE: Privatsphärenfördernde Gestaltung von Sicherheitsforschung und Sicherheitstechnik – Ein partizipativer Ansatz zur Entwicklung von akzeptablen und akzeptierten Prinzipien für die europäische Sicherheitsindustrie und Sicherheitspolitik

Gefördert im Rahmen der Preparatory Action for Security Research - PASR 2005, G.A. SEC5-SA-108600
Gesamtkosten: € 824.329
EU-Förderung: € 617.900
Projektbeginn: 01/02/2006
Projektdauer: 28 Monate

Koordinator:
Institut für Technikfolgen-Abschätzung
Österreichische Akademie der Wissenschaften

Kontakt:
Johann Cas
Tel: +43 1 51 581 6581
Fax: +43 1 710 98 83
E-Mail: jcas@oeaw.ac.at
WWW: prise.oeaw.ac.at

Partner:



Institut für Technikfolgen-Abschätzung (ITA), AT



Danish Board of Technology (DBT), DK



Unabhängiges Landeszentrum für Datenschutz (ULD), DE



Norwegian Board of Technology (NBT), NO

Kiel, den 25.5.2007

Teilnahme am PRISE Interview-Treffen am 15.6.2007 von 16 Uhr bis 19 Uhr

Information zum Interview-Treffen

Sie nehmen an unserer Bürgerbefragung im Rahmen des EU-Forschungsprojekts PRISE teil.
Wir zeichnen Ihre Wortbeiträge innerhalb der Gruppendiskussion auf.

Für die der EU-Kommission vorzulegende Studie über die Befragung sollen die Diskussionen anonymisiert als Anhang beigefügt werden. Dazu wird das ULD die Diskussionsbeiträge im Wortlaut abschreiben und dabei alle Bezüge (Namen, Beruf, Adresse, etc.) auf Ihre Person entfernen und durch einen Platzhalter ersetzen („Teilnehmer 1 bis 30“). Die Tonaufzeichnungen werden nach der Abschrift gelöscht. Eine andere als die beschriebene Verarbeitung der Wortbeiträge findet nicht statt.



Verantwortliche Stelle:
Unabhängiges Landeszentrum für Datenschutz (ULD)
Projekt PRISE
Projektleitung: Maren Raguse
Holstenstraße 98
24103 Kiel

Telefon: 0431 -988 1284
Fax: 0431 – 988 1223

Welche Meinung haben Sie zu Sicherheitstechnologien? Szenarien als Stoff zur Diskussionsanregung

Im Folgenden möchten wir Ihnen Geschichten von zwei Menschen - Carla und Peter - erzählen. Wir werden Ihre Begegnungen mit unterschiedlichen Sicherheitstechnologien und Maßnahmen beschreiben, und dabei ihre Gedanken und Ideen dazu erfahren. Um die Szenarien allgemein anwendbar zu machen, haben wir es vermieden, bestimmte Länder, Städte oder Flughäfen als Beispiele zu nennen. Stattdessen haben wir versucht zu zeigen, wie unterschiedliche Länder - und Sicherheitsbehörden - unterschiedliche Ansätze beim Einsatz von Sicherheitstechnologien gewählt haben. Die Szenen spielen sich in nicht allzu ferner Zukunft ab, um auch die Nutzung von einigen Sicherheitstechnologien oder gesetzlichen Bestimmungen zeigen zu können, die bisher noch nicht umgesetzt wurden.

Wir hoffen, dass die Geschichte dieser beiden Personen sie dazu anregen wird, über Sicherheit und den Schutz der Privatsphäre und Ihr Verhältnis zu diesen beiden Grundwerten nachzudenken.

Carla ist 62 Jahre alt. Sie hat ihr ganzes Leben gerne als Lehrerin gearbeitet, aber nun überlegt sie sich, in Pension zu gehen. Alles wird so technisch in diesen Tagen! Und auch die Kinder scheinen lauter zu sein als zuvor. Vielleicht wird sie einfach nur alt? Diese Woche wird sie sich darüber aber nicht den Kopf zerbrechen. Es ist der Beginn der Sommerferien und sie wird ihren Sohn, der in einem Nachbarland wohnt, besuchen.

Carla nimmt die U-Bahn, um zum Bahnhof zu fahren. Sie hat vorher ihre Universal-Fahrkarte aufgeladen. Sie verwendet diese zum Bezahlen ihrer Fahrten, indem sie sie vor ein Lesegerät beim Zugang zur U-Bahn hält. Die Universal-Fahrkarte aus Plastik enthält einen kleinen Chip. In ihm ist gespeichert, wie viele Fahrten noch als Restguthaben vorhanden sind. Carla hat sich für eine so genannte anonyme Universalkarte entschieden. Sie weiß, dass

die aufgeladenen Beträge verloren sind, wenn sie die Karte verliert; und es ist schon ein kleiner zusätzlicher Aufwand, eine eigene Karte dafür zu verwenden. Die normale Universal-Fahrkarte ist natürlich in die Mobiltelefone oder die neuartigen mobilen Multifunktionsgeräte des jeweiligen Besitzers integriert. Man muss es nur mit sich tragen und sich mit einem Fingerabdruck ausweisen, um alle Verkehrsmittel benutzen zu können.

Carla kann sich nicht helfen, aber sie empfindet es als unangenehm, Fingerabdrücke zu verwenden, um sich auszuweisen. Sie merkt, dass es die Jungen heute überhaupt nicht zu kümmern scheint, aber für sie wird es immer mit Verbrechen und Verhaftungen in Verbindung stehen. „Es ist schlimm genug, sich ausweisen und seinen Fingerabdruck hergeben zu müssen, wenn man ins Ausland reist, denkt sie sich.

Sie möchte dies keinesfalls öfter tun, als unbedingt notwendig!

Biometrische Verfahren

Biometrische Verfahren identifizieren Personen automatisch aufgrund ihrer biologischen Merkmale oder ihres Verhaltens. Biometrische Verfahren können verwendet werden, um Zugang zu Gebäuden oder zu Informationen (Computern, Daten) zu kontrollieren. Die am häufigsten gebrauchten Verfahren nutzen Fingerabdrücke oder Gesichtsmerkmale.

Der Vorgang, bei dem die biometrischen Merkmale einer Person mit den gespeicherten Daten verglichen wird, wird „matching“ genannt. Dieser Vergleich ergibt eine bestimmte Punktzahl. Ob eine Person akzeptiert oder abgelehnt wird, hängt davon ab, ob dieser Wert eine bestimmte Schwelle überschreitet.

Biometrische Merkmale können in Form des Originals oder als so genannte „Templates“ gespeichert werden. Das Template ist ein reduzierter digitaler Datensatz, der aus dem Original errechnet wird. Aus Datenschutzgründen wird empfohlen, nur das Template zu speichern und das Original zu löschen. Bei öffentlichen Systemen und Strafverfolgungsbehörden werden jedoch oft auch die Originalabbildungen aufbewahrt, etwa bei biometrischen Reisepässen oder Gesichtserkennungssystemen.

Wir können zwischen *Identifikation* und *Verifikation* unterscheiden. Bei der Identifikation geht es darum, herauszufinden, wer eine Person ist, indem ihre Merkmale mit allen in einer Datenbank gespeicherten Templates verglichen werden. Bei der Verifikation werden nur die Merkmale einer Person mit den über sie gespeicherten Werten verglichen; hier geht es darum, sicherzustellen, dass eine Person wirklich diejenige ist, als die sie sich ausgibt.

Eine Herausforderung für biometrische Systeme im Allgemeinen ist es, eine Balance zwischen der False Acceptance Rate (FAR) und False Rejection Rate (FRR) zu finden. Von falscher Annahme (oder falsch positiv) spricht man, wenn ein System eine Person fälschlicherweise identifiziert. Wenn das System hingegen eine registrierte Person nicht identifiziert, dann spricht man von, falscher

Ablehnung (oder falsch negativ).

Einer der wesentlichen Vorteile von biometrischen Verfahren ist, dass ein starker Bezug zur jeweiligen Person vorhanden ist. Biometrische Verfahren ermöglichen bessere Zugangskontrollen und Identitätsdiebstahl wird viel schwieriger, wenn persönliche Daten an die biometrischen Merkmale der Person gebunden sind. Dies ist auch der größte Nachteil biometrischer Systeme. Ist ein Satz von biometrischen Daten einmal geknackt, so ist er für immer verloren.

Peter ist 32 Jahre alt. Er arbeitet als Vertreter für ein Autohaus. Heute steht er früh auf, um zu einer Automobilmesse in Mitteleuropa zu reisen. Er duscht sich schnell, nimmt seine Tasche und steigt dann in sein Auto, um zum Flughafen zu fahren. Wie üblich ist er zu spät dran, da er aber für den Quick-Check-In registriert ist, sollte es kein Problem geben. Beim Quick-Check-In erspart man sich das ganze Theater mit dem Herzeigen seines Reisepasses und mit der Überprüfung, ob man ein gesuchter Verbrecher ist und natürlich auch die ganzen rigorosen Sicherheitsüberprüfungen. Man muss sich nur einmal einer sehr gründlichen Überprüfung und Registrierung unterziehen und zustimmen, dass alle Daten am Flughafen gespeichert werden. Im Gegenzug kann man das ganze normale Check-In Verfahren umgehen und sich nur mehr am Eingang biometrische verifizieren lassen.

Peter muss an seinen Kollegen denken, für den seiner Meinung nach der Schutz der Privatsphäre zu einer fixen Idee geworden ist. Er behauptet, dass es schon jetzt zu viel Überwachung in der Gesellschaft gibt, und er akzeptiert nicht einmal Cookies auf seinem Computer! Sogar die Google Toolbar hat er deinstalliert - niemand tut das! Wenn es wahr wäre, dass amerikanische Behörden diese Daten nutzen, um soziale Vernetzungen herauszufinden und nach verdächtigen

Profilen zu suchen, dann wäre das doch bestimmt allgemein bekannt? Wahrscheinlich ist er schon ein paar Stunden früher aufgestanden und steht nun in der Menschengänge vor der Sicherheitsüberprüfung. Nun gut, er hat es ja so gewollt! Peter hofft nur, dass es sein Kollege schafft, rechtzeitig durch die Sicherheitskontrollen zu kommen, damit sie noch einmal ihre Präsentation durchgehen können, bevor sie ins Flugzeug einsteigen müssen.

- o -

Carla kommt am Hauptbahnhof an. Wie in der U-Bahn gibt es auch hier überall Kameras. Bildschirme und Lautsprecher wiederholen Sicherheitswarnungen, bis sie niemand mehr bewusst wahrnimmt: "Abgestellte Taschen werden von den Sicherheitskräften entfernt!" oder „Ihr Gesicht wird automatisch mit jenen von bekannten Terroristen verglichen!" Über die zweite Meldung gab es vor einigen Jahren eine Debatte. Die meisten Länder geben nicht bekannt, dass sie Gesichter erfassen und mit unterschiedlichen Datenbanken abgleichen; und es wurde vorgeschlagen, dass man es auch hier nicht tun sollte. Aber die Regierung war sich einig, dass die Leute grundsätzlich wissen sollten, wann und wo sie überprüft werden. "Das ist besonders wichtig, wenn man selbst nicht mehr feststellen kann, ob Kameras installiert sind oder nicht" denkt sich Carla. Sie hat gehört, dass es Länder geben soll, wo sie auch die E-Mails und die Telefongespräche auf verdächtige Wörter und Sätze überprüft werden, aber das kann bestimmt nur ein Gerücht sein!

Carla fühlt, dass der ganze Lärm ihr in den Kopf steigt und steuert auf die *stille Zone* zu. Sie muss ihre Identitätskarte herzeigen, ehe sie eintreten kann, aber nachdem sie erst einmal drinnen ist, entspannte sie sich. "Keine Kameras, keine Mobiltelefone, keine Computer, keine störenden Warnungen! Es sollte wirklich mehr solche

technikfreie Zonen geben ", denkt sie sich.

Es ist nicht so, dass sie nicht an Kameras gewöhnt wäre. Schließlich gibt es sie schon die meiste Zeit, seitdem sie erwachsen ist, aber sie scheinen in letzter Zeit immer aufdringlicher zu werden? Nachdem man begonnen hatte, sowohl Gesichtserkennungssoftware als auch Programme zum Erkennen verdächtigen Verhaltens einzusetzen, fühlt sie sich mehr beobachtet und überwacht als zuvor: "Bewege ich mich jetzt wie eine Terroristin?" Wie peinlich wäre es, etwas zu tun, das die Antiterrorpolizei veranlassen könnte, sie aufzugreifen und zu überprüfen! Um fair zu sein, dies ist ihr noch nie tatsächlich passiert, aber sie kann nicht anders, als darüber nachzudenken, wenn sie von Kameras umgeben ist.

Und, wie die meisten Leute, kennt sie jemanden, der tatsächlich verdächtigt worden ist, ein Terrorist zu sein. Als diese Sicherheitstechnologien eingeführt wurden, gab es viele Probleme mit Gesichtserkennungssystemen. Und weil die Politik die Möglichkeit und den damit verbundenen Skandal vermeiden wollte, dass eine Person auf den Fahndungslisten unerkannt durch die Kontrolle schlüpft, war das Ergebnis eine große Anzahl von Fehlalarmen (*falsch Positive*).

Einer ihrer Kollegen, dessen Eltern aus dem Iran stammen, wurde mit einem Terroristen verwechselt. Er empfand diese Verwechslung als sehr demütigend. Und sie kann das auch gut verstehen, wenn er sagt: "Wenn man von Antiterrorereinheiten in kugelsicheren Westen festgenommen wird und aussieht wie ich, sehen dich die Leute danach mit anderen Augen an -, selbst wenn man mit einer Entschuldigung wieder freigelassen wird". Carla weiß, dass er für eine Weile danach Orte mit Videoüberwachung mied, insbesondere wenn er mit seinen Kindern unterwegs war.

In jüngster Zeit haben mehr und mehr

Personen die Legitimität und Wirksamkeit der Videoüberwachung bezweifelt. In einigen Stadtteilen haben sie mit Versuchen begonnen, anstelle von Überwachungskameras eine bessere und hellere Straßenbeleuchtung zu installieren. Offensichtlich mit guten Ergebnissen!

- o -

Da er in einem Autohaus arbeitet, kann Peter immer die neuesten Modelle fahren. Das Auto, das er im Moment benutzt, ist mit neuester Technik ausgestattet: einem Galileo Satellitennavigationssystem,

Videoüberwachung

Von Videoüberwachung mit *aktiven Kameras* spricht man, wenn die Person, die die Vorgänge am Monitor beobachtet, die Kamera durch Bewegen oder Zoomen steuern kann, um einer Person oder einer sich abzeichnenden Situation folgen zu können. Aktive Kameras können mit automatisierten visuellen Überwachungsprogrammen kombiniert werden, die komplizierte Verfahren verwenden, um verdächtiges Verhalten zu erkennen oder Personen anhand von in Datenbanken gespeicherten Fotos zu identifizieren.

Passive Kameras: Diese Kameras zeichnen auf, was in einer bestimmten Stelle (zum Beispiel in einem Kiosk) geschieht. Die Aufzeichnungen werden nur dann betrachtet, wenn es besondere Vorfälle gibt, etwa einen Raub, Kampf usw.

Während die früheren Videoüberwachungssysteme analoge Technik nutzten, werden sie zunehmend durch digitale Systeme ersetzt. Mit diesen Systemen kann man schneller nach bestimmten Ereignissen suchen oder verdächtige Personen mit Hilfe von vorhandenen Datenbanken identifizieren. Es besteht aber die Sorge, dass digitale Aufzeichnungen auch leichter manipuliert werden können.

Automatische Gesichtserkennung

Bei automatischen Gesichtserkennungssystemen wird das Gesicht einer Person automatisch erfasst und mit in einer Datenbank gespeicherten Informationen zur Identifikation oder Zugangskontrolle verglichen. Solche Systeme werden

normalerweise verwendet, um sicherzustellen, dass eine Person beispielsweise nicht auf einer Liste von bekannten Verbrechern oder Terroristen ist.

Automatische Kennzeichenerfassung

Diese Systeme werten die von Videokameras erfassten Autokennzeichen aus und vergleichen sie mit einer Datenbank. Systeme zur Kennzeichenerkennung werden in mehreren Ländern eingesetzt. Hauptsächlich werden sie verwendet, um Mautvergehen oder Geschwindigkeitsübertretungen zu verfolgen, aber sie werden auch verwendet, um gestohlene Fahrzeuge zu identifizieren.

automatischem Notruf über das eCall-System und einer Reihe von weiteren Fahrzeugsicherheitssystemen. Peter weiß nicht einmal genau, was diese alles können. Das eCall-System ist jetzt in alle neuen Autos standardmäßig eingebaut, und es soll automatisch einen Notruf absetzen, wenn das Auto in einen Unfall verwickelt ist. Weil es das Galileo-System nutzt, kennt es die genaue Position des Autos.

In den letzten Jahren hat es viele Vorschläge gegeben, dieses System auch für andere Zwecke zu verwenden. Nach einem versuchten Terrorangriff in Berlin stahlen die Terroristen ein Auto und flüchteten damit durch Deutschland. Es zeigte sich, dass das System verwendet werden konnte, um Autos aufzuspüren und sogar zu stoppen! Da das gestohlene Auto ein teures Modell mit dem neuesten Stand an Antidiebstahlstechnik war, konnte es einfach mit einem über Satelliten ausgestrahlten Befehl gestoppt werden. Die Terroristen konnten festgenommen werden; danach beschlossen die EU-Mitgliedsstaaten, dass diese Systeme auch von der Polizei für die Verfolgung von Verbrechern und verdächtigen Terroristen verwendet werden können.

Nach genauen Untersuchungen, wie viele Verkehrstote man vermeiden könnte, wenn die Fahrer die Geschwindigkeitsbegrenzungen einhalten

würden, wurde vorgeschlagen, in Fahrzeugsicherheitssysteme auch eine automatische Geschwindigkeitskontrolle einzubauen. Dieses Modul kann die jeweils erlaubte Höchstgeschwindigkeit mit dem tatsächlich gefahrenen Tempo vergleichen. Der ursprüngliche Vorschlag ging so weit, dass ein Chip im Motor dafür sorgen sollte, dass kein Auto schneller als die erlaubte Höchstgeschwindigkeit fahren kann. Nach heftigen Protesten von Seiten der Automobilindustrie und von Automobilclubs wurde davon abgesehen. Im Moment ist das System so eingestellt, dass jedes Mal wenn ein Auto zu schnell fährt, ein Anruf an die Zentrale der Verkehrspolizei erfolgt, und die Geldstrafe automatisch vom Bankkonto des Autoeigentümers abgebucht wird.

Peter steigt aufs Gaspedal. Noch sind nicht alle Straßenabschnitte vom System erfasst. Er hat eine Liste der freien Strecken heruntergeladen und in sein Navigationssystem eingespeichert. Er bekommt jedes Mal, wenn er auf einer unkontrollierten Strecke unterwegs ist, ein Signal. Er wird auch gewarnt, wenn er sich wieder an Geschwindigkeitsbegrenzungen halten muss. "Es ist gut, dass Überwachung auch in umgekehrter Weise funktioniert", denkt er sich.

Peter kommt am Flughafen an. Das Nummernschild seines Autos ist schon im System gespeichert und sein Auto wird automatisch registriert, wenn er in das

Technologien zur Ortung

Es ist möglich, die ungefähre Position von Mobiltelefonen aus den Koordinaten der nächstgelegenen Funkstationen zu berechnen.

Für eine genauere Ortung werden satellitenbasierte Systeme genutzt:

GPS ist das derzeit vorhandene System, die Abkürzung steht für *Global Positioning System*. Es besteht aus 24 Satelliten, die die Erde umkreisen. Mit den Signalen von drei Satelliten kann man den Längen- und Breitengrad des

GPS-Empfängers bestimmen, mittels vier Satelliten kann man auch die Höhe berechnen.

Das zukünftige System heißt *Galileo* und wird 30 Satelliten umfassen, die genaueste Orts- und Zeitinformationen für Benutzer am Boden und in der Luft bieten werden. Es soll im Jahr 2010 betriebsbereit sein. Es wird genauer als das GPS-System sein, und soll auch innerhalb von Gebäuden funktionieren.

eCall

Das eCall-System soll in Autos eingesetzt werden. Das Gerät enthält Sensoren, die es nach einem Unfall aktivieren. Es löst einen automatischen Notruf aus und übermittelt Information über die Zeit, den genauen Standort und das betroffene Fahrzeug.

Das Gerät wird nicht permanent mit einem mobilen Datenübertragungsnetz verbunden sein, es verbindet sich nur, nachdem es aktiviert worden ist. Es gibt jedoch Befürchtungen, dass sich dies ändern könnte: ein Beispiel wäre das permanente Senden von weiteren Daten, etwa für Versicherungsgesellschaften. Sorgen bereitet auch ein möglicher unbefugter Zugang zu Datenbanken, in denen eCall-Daten gespeichert werden. Ab September 2009 werden alle neuen Autos in den teilnehmenden Ländern mit eCall-Geräten ausgerüstet sein.

Parkhaus fährt. Es ist dieselbe Technik, die in den Städten verwendet wird, um gestohlene Fahrzeuge zu identifizieren. Er dachte eigentlich, dass solche Systeme überflüssig werden, nachdem das eCall-System mit Galileo-Satellitenavigation eingeführt wurde. Offensichtlich wissen aber organisierte Banden genau, wie das System ausgeschaltet werden kann. Und er weiß, dass in einigen Ländern sogar gefordert wird, dass der Fahrer selbst in der Lage sein sollte, das eCall-System zu deaktivieren. Solche Forderungen bringen immer Schwierigkeiten für die Autoindustrie mit sich! Und warum ist es so, dass die Kriminellen der Technik immer einen Schritt voraus zu sein scheinen?

Zweckentfremdung

Datenbanksysteme sind gegenüber Zweckentfremdungen anfällig, darunter

versteht man die Verwendung von Daten für andere Aufgaben als ursprünglich geplant. Ein Beispiel dafür ist die norwegische Datenbank über Asylantragsteller, die auch biometrische Informationen wie Fingerabdrücke enthält. Sie wurde der Polizei für Ermittlungen bei strafbaren Handlungen zur Verfügung gestellt. Der ursprüngliche Zweck der Datenbank war es, die Identität von Asylanten zu verifizieren.

Er parkt das Auto, steigt aus und steuert auf den Quick-Check-In für sein Terminal zu. Er hält seinen Finger auf den Sensor und schaut direkt in die Kamera. Ein grünes Licht leuchtet auf, und die Tür öffnet sich.

Obwohl die Sensoren für Fingerabdrücke viel besser sind, als sie es früher waren, haben einige Leute immer noch Schwierigkeiten, diese zu verwenden: Sein Großvater ist so ein Beispiel. Obwohl er eigentlich ein sehr rüstiger achtzigjähriger Mann ist, wird er zunehmend isoliert. Heutzutage muss man sich bei allen möglichen Gelegenheiten Fingerabdrücken ausweisen. Er ist des ganzen Theaters und Ärgers überdrüssig, den man über sich ergehen lassen muss, wenn die eigenen Fingerabdrücke nicht von Sensoren gelesen werden können. Daher bleibt er oft lieber gleich zuhause.

Peter geht manchmal zur Bibliothek, um sich *echte* Bücher auszuleihen. Er schmunzelt, wenn er daran denkt, wie sein Bibliotheksprofil aussehen muss. Wenn Nachrichtendienste es jemals bei der Suche nach verdächtigen Personen analysiert hat, könnte sie sich gefragt haben, warum ein dreißigjähriger Mann sich Bücher wie "Dating für Senioren" oder "Unsere Freunde, die Vögel" ausborgt.

Vor einigen Jahren, direkt nachdem ein größerer Terrorangriff in den USA verhindert werden konnte, wurde tatsächlich vorgeschlagen, dass Sicherheitsbehörden alle möglichen Datenbanken durchsuchen dürfen sollten. Und das betraf nicht nur vermutliche

Verbrecher oder Terroristen. Sie wollten alle Daten, von Bibliotheken, Elektrizitäts- und Gasverbrauchsmustern, Verkehrsdaten für das Telefon und das Internet, Reisen bis hin zu Einkaufsgewohnheiten, analysieren. Durch das Suchen nach verdächtigen Mustern wollten sie mögliche Terroristen identifizieren.

Sein Kollege Alex war damals sehr empört gewesen, und Peter hatte versucht, mit ihm zu diskutieren: Bestimmt würden sie diese Maßnahmen nicht ergreifen, wenn sie nicht gute Gründe dafür hätten? Und die Behörden sollten doch tun, was auch immer sie können, um Terroristen zu fangen? Alex war davon nicht überzeugt, und meinte, dass zumindest anonymisierte Daten für diese Analysen verwendet werden sollten: "Wenn sie etwas verdächtig finden, können sie sich ja über einen Gerichtsbeschluss die wahre Identität aufdecken lassen. Es gibt keinen wirklichen Grund, warum sie alles über jeden wissen sollten!"

Peter war nicht wirklich daran interessiert gewesen, das Thema weiter zu diskutieren, aber sein Kollege sprach ihn in jeder Mittagspause immer wieder darauf an, und schlussendlich hatte er eine Petition gegen den Vorschlag unterschrieben. "Aber eigentlich verstehe ich die Aufregung nicht wirklich", sagte er zu sich. "Bestimmt ist dies nur ein Problem für jene, die etwas zu verbergen haben?" Andererseits erappte er sich dabei, sich selbst zu fragen, ob es irgendwo gespeichert worden ist, dass er diese Petition unterschrieben hat.

Total Information Awareness (TIA)

TIA war ein Programm der DARPA (Defence Advanced Research Projects Agency) der US-Regierung. Es lässt sich am ehesten mit dem Begriff "allumfassende Auswertung von Informationen" übersetzen. Das TIA-Programm umfasste drei Kategorien von Software-Werkzeugen: automatische Sprachübersetzung, Suchmaschinen und Mustererkennung sowie fortgeschrittene Systeme zur Entscheidungs-

findung.

Das Ziel von TIA war es, terroristische Angriffe vorhersagen zu können, ehe sie eintreten. Es war beabsichtigt, dass das System private und öffentliche Datenbanken wie auch das Internet nach verdächtigen Daten durchsucht, die auf einen Terroristenangriff hinweisen könnten. Im September 2003 wurde die Finanzierung von TIA vom US-Kongress gestoppt, aber viele der Projekte innerhalb des Programms werden unter anderem Namen weitergeführt.

Carla bleibt eine Weile in der stillen Zone sitzen und liest ihr Buch. Dann macht sie sich auf den Weg zum Sicherheitscheck.

Eine Folge der zunehmenden Forderung nach Kontrollen war es, dass Sicherheitsgates nicht nur an Flughäfen, sondern auch im internationalen Zugverkehr und vielen anderen Orten, an denen viele Personen zusammenkommen, eingerichtet wurden. Sie weiß, dass es in einigen Ländern sogar bei den Eingängen von Einkaufszentren und in Sporthallen Sicherheitschecks gibt. Vor einigen Jahren konnte ein Selbstmordattentäter am Eingang eines Einkaufszentrums, nahe an dem Ort, wo ihr Sohn wohnt, festgenommen werden. Anscheinend hatten sie gerade begonnen, eine neue Technologie zum Durchleuchten einzusetzen, von der der Attentäter noch nichts wusste. Dennoch ist sie froh, dass man in ihrem Land nicht so weit gegangen ist. Bislang werden die Passagiere nur auf Flughäfen und auf Bahnhöfen durchleuchtet.

Sie selbst macht sich keine Sorgen über die Sicherheit in Einkaufszentren; soweit sie weiß, hat es in ihrem Land bislang noch keine einzige Bedrohung in diesem Bereich gegeben. Aber sie hat Statistiken gesehen, die zeigen, dass mehr Leute dazu übergehen, in den kleineren Läden in den Stadtzentren einzukaufen; die Einkaufszentren behaupten, dass sie

Einnahmeverluste erleiden müssen, weil es ihnen nicht erlaubt wird, neue Scannertechnologien wie die „Nackte Maschine“ einzusetzen.

Carla nimmt ihren Reisepass heraus und geht zum Irisscanner. Sie weiß, dass einige Länder immer noch Fingerabdrücke in ihren Ausweisen und Reisepässen verwenden, aber sie meint, dass es sicherer ist, die Iris zu benutzen. Das Lesegerät vergleicht ihre Iris mit den in ihrem Reisepass gespeicherten Daten. Sie war beunruhigt darüber, aber ihr Sohn, der in der Informationstechnikindustrie arbeitet, hat ihr versichert, dass es jetzt völlig sicher sei. "Die ursprüngliche Verschlüsselung im ersten Reisepass war ziemlich schwach", sagte er, "aber mit der jetzt verwendeten Verschlüsselung würde ein Supercomputer Tausende von Jahren brauchen, um die Verschlüsselung zu knacken! Dazu kommt noch, dass in den frühen Reisepässen die tatsächliche Abbildung des Gesichts, der Fingerabdrücke oder der Iris gespeichert wurden. Jetzt speichern sie diese Daten nur mehr in Form von Templates - reduzierten digitalen Datensätzen, welche die wichtigsten Merkmale der Iris und des Gesichts enthalten. Selbst wenn es gelänge,

Funketiketten (RFID)

RFID (Radio Frequency Identification) ist eine Technologie zur automatischen Identifikation unter Verwendung von Radiowellen. Winzige integrierte Schaltungen (Chips), welche die Informationen enthalten, werden in Dokumenten eingebettet oder in Produkte integriert. Mittels eines Lesegeräts können die Informationen von allen Funketiketten innerhalb eines bestimmten Bereichs abgerufen werden.

RFID-Etiketten oder Tags, wie sie ihn Englisch bezeichnet werden, gibt es sowohl in *aktiver* als auch *passiver* Form. Aktive Tags werden zum Beispiel eingesetzt, um die Mautgebühren für LKWs automatisch abzubuchen. Sie enthalten eine Batterie und können daher mehr Informationen speichern und auch aus größeren Distanzen gelesen werden. Passive Tags enthalten keine Batterie, sie entnehmen die

benötigte Energie direkt aus dem Radiosignal, das vom Lesegerät ausgesendet wird. Eine typische Anwendung von passiven Tags ist der neue europäische Reisepass.

Die meisten Tags stellen ihre Informationen jedem Lesegerät in der Nähe zur Verfügung; es gibt aber auch Tags, die eine Passwort verlangen oder andere Formen der Zugangskontrolle eingebaut haben.

Biometrischer Reisepass

Ein biometrischer Reisepass besteht aus dem normalen Dokument mit einem zusätzlich eingebetteten RFID-Chip.

Der Chip enthält obligatorische und optionale Daten. Außerdem gibt es eine Photographie des Besitzers als visuelle Verknüpfung zwischen dem Besitzer und dem Reisepass.

Die Internationale Zivilluftfahrtorganisation (International Civil Aviation Organization - ICAO) hat einen Chip für den Reisepass ausgewählt, der über Funk ausgelesen werden kann (RFID). Das *Gesicht* wurde von der ICAO bei Reisepässen als biometrisches Hauptmerkmal ausgewählt; *Fingerabdrücke* und *Iris* werden als weitere, sekundäre biometrische Merkmale empfohlen. Die europäische Union hat nur Fingerabdrücke als sekundäres Merkmal ausgewählt.

Biometrische Reisepässe haben viele Debatten hervorgerufen, insbesondere im Zusammenhang mit der Sicherheit der biometrischen Informationen. Es wird befürchtet, dass die im Chip gespeicherten biometrischen Informationen ohne Wissen des Eigentümers gestohlen werden könnten, indem der Datenaustausch belauscht oder heimlich Lesegeräte in die Nähe gebracht werden.

Um diese Sorgen auszuräumen, ist ein System zum Schutz des Zugangs (Basic Access Control - BAC) entwickelt worden. Bei BAC benutzt das Kontrollsystem einen „Schlüssel“, der aus den frei zugänglichen Daten (dem Strichcode) abgeleitet wird, um den Chip zu entsperren und auslesen zu können. BAC ist als nicht sicher genug kritisiert worden; tatsächlich ist es Sicherheitsexperten innerhalb von kurzer Zeit gelungen, die Verschlüsselung zu brechen.

die Verschlüsselung zu knacken, wäre es damit nicht möglich, das Gesicht oder die Iris nachzubilden, um den Passinhaber zu

imitieren."

Ihr ist auch zugesichert worden, dass das Lesegeräte ihr Iris-Abbild nur verwendet, um es mit dem im Reisepass gespeicherten Template vergleichen zu können, und dass es nicht in einer zentralen Datenbank gespeichert wird. Sie ist sich nicht so sicher, was geschieht, wenn ihr Reisepass an ausländischen Grenzen kontrolliert wird. Werden dort die Daten auch nach dem Vergleich gelöscht?

Sie erinnert sich daran, dass es vor einigen Jahren einen Skandal mit einer zentralen Fingerabdruckdatenbank gab – war es in den USA? Viele Fingerabdrücke wurden von einem Angestellten gestohlen und an eine internationale Verbrecherorganisation verkauft. Tausenden von Menschen wurde dadurch ihre Identität gestohlen und sie erlebten viele Arten von Problemen - etwa dass sie bei Grenzkontrollen in den Fahndungslisten erschienen, oder ihre Bankkonten geleert wurden. Besonders schwierig war es, weil es sehr lange dauerte, ehe die Regierung eingestand, dass Daten verloren gegangen waren. Und in der Zwischenzeit wollte ihnen niemand glauben, dass ihre Identitäten gestohlen worden waren - oder dass es überhaupt möglich war, die Fingerabdrücke von jemandem zu verwenden, um seine Identität zu stehlen!

Carla weiß das aber besser. Letzten Sommer wurde einem Freund ihres Sohns sein Personalausweis gestohlen, kurz bevor er und seine Familie in Urlaub fahren wollten. Er fürchtete, dass sie alles würden abrechnen müssen, weil seine Identität als gestohlen aufgelistet sein würde. Offensichtlich kann aber das Schengen Informationssystem, das in vielen europäischen Ländern verwendet wird, Personen berücksichtigen, deren Identität gestohlen wurde. Daher konnten er und seine Familie wie geplant reisen, und er wurde nie für einen Verbrecher oder ein Terrorist gehalten, obwohl sein neu

ausgestellter Personalausweis wahrscheinlich gründlicher überprüft wurde als der eines durchschnittlichen Reisenden.

Nach der Identitätsüberprüfung wird Carlos Gepäck durchleuchtet, bevor sie selbst durch etwas gehen muss, dass als die *nackte Maschine* bezeichnet wurde. Sie ist erleichtert, dass die wirkliche „nackte Maschine“ in ihrem Land niemals auf Flughäfen oder Bahnhöfen eingesetzt wurde.

Personenscanner („Nackte Maschine“)

Röntgen- oder Terrahertzstrahlen können Materialien durchdringen. Sie können daher auch für die Entdeckung und Darstellung von unter der Kleidung verborgenen Gegenständen verwendet werden.

Ein Personenscanner nutzt diese Technik, um zu erkennen, ob eine Person Waffen oder Sprengstoffe an ihrem Körper versteckt hat. Es gibt sehr unterschiedliche Systeme; manche offenbaren alles unter der Kleidung - nicht nur Waffen oder Sprengstoffe - daher stammt auch aus dem Englischen übernommene Name „**Nackte Maschine**“ (naked machine). Diese Art der Sicherheitstechnologie ist am Londoner Flughafen Heathrow (Terminal 4) seit 2004 getestet worden. Andere Systeme nehmen Bilder von verborgenen Objekten auf und projizieren sie auf eine geschlechtslose Puppe.

Die Sicherheitsbehörden haben verschiedene Systeme bewertet, und entschieden, dass es genauso so sicher war, ein Modell zu kaufen, bei dem unter der Kleidung versteckte Sachen auf einer geschlechtsneutralen Puppe abgebildet werden.

Obwohl sie schon 62 ist, ist Carla immer noch wegen ihres Körpers befangen, und sie ist froh, dass die jungen Männer am Sicherheitsgate sie nicht nackt zu sehen bekommen. Sie muss ihre Schuhe ausziehen, aber davon abgesehen hat sie keine Probleme und sitzt bald bequem im Zug.

- o -

Peter eilt durch die Flughafenhalle zur Sicherheitskontrolle. Natürlich müssen sogar die Quick-Check-In-Kunden sich einer Form der Sicherheitsüberprüfung unterziehen, aber sie haben einen eigenen Zugang, und es sind nur Vielflieger darunter. Niemand vergisst hier einen Gürtel mit Metallschnalle abzulegen, oder ist dumm genug, Kleingeld in den Taschen zu lassen. Und es ist schon Jahre her, dass Businesschuhe noch Metallteile enthielten. Er schluckt kurz und geht durch die *nackte Maschine*. "Warum muss es hier immer so kalt sein?" denkt er sich, und errötet, als er bemerkt, dass eine der Wachen eine Frau in seinem Alter ist.

Vorratsdatenspeicherung

Eine Datenbank ist eine organisierte Sammlung von Daten. Es wird allgemein anerkannt, dass man wesentlich mehr über eine Person erfahren kann, wenn Daten aus verschiedenen Quellen zusammengefügt werden als wenn diese Daten jeweils einzelnen betrachtet werden. Es ist daher ein wichtiges Prinzip des Datenschutzes, das in Datenbanken jeweils nur jene Informationen gesammelt werden dürfen, die für den Zweck dieser Datenbank notwendig sind, und dass die Daten gelöscht werden sollen, sobald sie nicht mehr benötigt werden.

In letzter Zeit ist ein Trend zu beobachten, nach dem Regierungen mehr Daten als für den ursprünglichen Zweck erforderlich sind, speichern wollen und unterschiedliche Datenbanksysteme für Sicherheitszwecke zusammenführen wollen. Zumeist sind Daten aus dem Bereich Informations- und Kommunikationstechnologien, wie Kommunikationsverkehrsdaten von Telefonen, Mobiltelefonen und Internetnutzung gemeint, wenn die Einführung von Vorratsdatenspeicherung diskutiert werden.

Die EU hat eine Richtlinie über die Vorratsdatenspeicherung erlassen. Daten darüber, wer mit wem, wann und wo kommuniziert hat, werden gespeichert, aber nicht der Inhalt der Kommunikation. Diese Daten können bis zu zwei Jahre lang aufbewahrt werden.

Verschiedene Behörden in den USA haben berichtet, dass sie im Jahr 2005 persönliche Daten von kommerziellen Datensammlern im Wert von \$ 30 Millionen gekauft haben. Diese Agenturen sammeln und verknüpfen Daten aus unterschiedlichen Quellen und verkaufen diese an ihre Kunden. Die Quellen können öffentliche Datenbanken sein, Informationen übers Internet frei verfügbar sind oder Daten, die im privaten Eigentum sind, z.B. von Privatunternehmen.

Dennoch begrüßt er es, dass am Flughafen die *wirklich* nackte Maschine eingesetzt wird. Irgendwie fühlt er sich sicherer dabei.

Peter bemerkt eine zusätzliche Sicherheitseinrichtung, die er zuvor noch nie gesehen hat. Nach der nackten Maschine befindet sich ein zweites "Tor"; manche der Passagiere werden aufgefordert, durch dieses durchzugehen. Er erinnert sich vage daran, gehört zu haben, dass ein neues Sicherheitssystem in diesem Flughafen getestet werden soll. Dieses erfasst angeblich Daten wie die Körpertemperatur, Schweiß, Pulsfrequenz usw. Fakten, die ein Zeichen für Krankheiten wie SARS oder eine Vogelgrippe sein könnten oder anzeigen können, dass eine Person nervös ist. Manche der Testpersonen werden in ein Verhörzimmer in der Nähe geführt. Er ist froh, dass er nicht für den Test ausgewählt wurde, selbst wenn er gesund ist und ein reines Gewissen hat. "Ist es angebracht, diesen Test hier durchzuführen? Wissen sie nicht, dass die Leute, die das Quick-Check-In verwenden, es eilig haben?"

Er geht zum Gate und setzt sich hin. Vielleicht sollte er Yasmin anrufen und ihr sagen dass er kommt? Sie arbeitet für den Autohersteller, den sein Autohaus vertritt, er hat sie bei der letzten Autoausstellung, die er besuchte, kennengelernt. Sie verstanden sich vom ersten Moment an sehr gut, und er würde sie gerne wieder sehen. Andererseits zögert er, sie mit seinem Handy anzurufen. Er weiß, dass

Yasmins Bruder in einer Jugendgruppe in seiner Moschee sehr aktiv ist und dass Yasmin wahrscheinlich auf irgendeiner Art als Teil des Netzwerks ihres Bruders überwacht wird. Es tut ihm leid, dass er nicht, als er das letzte Mal in Asien war, einige anonyme Telefonwertkarten gekauft hatte. Es ist nicht mehr erlaubt, solche Karten in Europa zu verkaufen.

Abhören

Unterschiedliche Technologien können genutzt werden, um die Aktivitäten und Kommunikation von Bürgern im Internet, beim Telefonieren oder in bestimmten Gebieten zu belauschen. Eine bekannte Form ist das Abhören von Telefongesprächen. Dabei wird ein Abhörgerät in Telefonzentralen installiert, das Abhörgerät kann die Gespräche des Verdächtigen erfassen oder auch gegen Telefone von Personen gerichtet werden, von denen man annimmt, dass der Verdächtige sich an sie wenden wird.

Eine erweiterte Version des Abhörens erfasst unterschiedslos alle Kommunikationsmöglichkeiten (Telefon, Mobiltelefon, Internet), die auf verdächtige Aktivitäten untersucht werden. Ein Beispiel dafür ist das Echelon Netzwerk, das von einem Bündnis zwischen den USA, Großbritannien, Kanada, Australien und Neuseeland betrieben wird. Das System wurde ursprünglich zur Überwachung der Kommunikation in der Sowjetunion und in Osteuropa eingesetzt. Kommunikationsmuster können analysiert werden und Inhalt kann nach bestimmten Stichwörtern durchsucht werden.

Er will auch nicht das Internet nutzen. Wer weiß, was hier am Flughafen alles protokolliert wird? Er ist sich nicht einmal sicher, welche Regeln heutzutage gelten. Hat die Polizei direkten Zugang zu diesen Arten von Daten oder brauchen sie eine richterliche Vollmacht? Er denkt sich plötzlich, dass er die Debatte über den Schutz der Privatsphäre besser verfolgen hätte sollen. Er wird bestimmt seinen Kollegen fragen, wenn dieser ins Flugzeug einsteigt.

Das letzte Mal, als er mit Yasmin ausging,

erwähnte sie, dass sie sich sicher war, dass ihre E-Mails abgehört werden, und sie bat ihn darum, ein Verschlüsselungsprogramm zu verwenden, wenn er ihr schreiben wollte. "Eine unverschlüsselte E-Mail ist wie eine Postkarte", erklärte sie. "Jeder, der Zugang zu ihr bekommt, kann sie lesen - hast du das nicht gewusst?"

Eigentlich wollte er ihr schreiben. Aber er musste feststellen, dass das E-Mail-Programm, das sie im Büro verwenden, keine Verschlüsselung integriert hat, und er war noch nicht dazu gekommen, ein anderes Programm zu installieren. Er hofft, dass sie ihm nicht böse ist, dass er sich die ganze Zeit nicht gemeldet hat. "Ich werde es ihr erklären, wenn wir uns treffen", denkt er sich.

Es ist Zeit, ins Flugzeug einzusteigen. Er geht ans Gate, drückt seinen Finger auf den Sensor und geht als einer der ersten Passagiere an Bord. Es gibt noch mehr als genug Platz für das Handgepäck. Er denkt an seinen Kollegen, der wahrscheinlich immer noch in der Schlange vor der Sicherheitskontrolle steht, bevor er sich zurücklehnt und seine Augen schließt.

- o -

"Mama ist schon auf dem Weg", sagt Carlos Sohn zu seiner Frau, nachdem er eine Nachricht auf seinem Mobiltelefon erhalten hat. "Sie sollte in drei Stunden hier sein." Seine Mutter weiß es nicht, aber das neue Mobiltelefon, das er ihr zu Weihnachten geschenkt hat, ist mit einem *Friend Finder* genannten Dienst verbunden. Diese Technik ist eine neue Version der Peilsender, wie man sie aus alten Kriminalfilmen kennt. Hier konnte man einen Verdächtigen als kleinen Punkt auf einer Landkarte verfolgen. Der Hauptunterschied ist, dass heute dazu das im Mobilgerät integrierte Galileo-System genutzt wird. Er kann dadurch die Bewegungen seiner Mama auf einer Landkarte verfolgen,

Technologien zur Förderung der Privatsphäre

Technologien, die direkt dazu beitragen, die Privatsphäre zu schützen, werden als privatsphärenfördernde oder privatsphärenfreundliche Technologien bezeichnet.

Anonymisierung ist ein Beispiel dafür. Es gibt Dienste, die eine anonyme elektronische Kommunikation für normale Benutzer ermöglichen. Dabei werden die Verbindungen zwischen Nutzen und die Spuren, die sie hinterlassen versteckt, damit kann eine unerwünschte Identifizierung verhindert werden. Bezahlungsunmittelbarkeit oder die Nutzung von nicht registrierten Wertkarten sind traditionelle Mittel, die Anonymität bereitstellen.

Identitäts-Management ist auch eine Form privatsphärenfördernder Technologien: In einigen Fällen wollen Sie sich vielleicht nicht identifizieren, sondern ein Pseudonym (zum Beispiel bei Foren im Internet) verwenden. Um die Verknüpfung von Daten schwieriger zu machen, kann es nützlich sein, verschiedene Benutzernamen (die Ihre Identität nicht zeigen) und Passwörter für verschiedene Zwecke zu verwenden. Identitätsmanagementsysteme helfen Ihnen dabei, Ihre verschiedenen Benutzernamen und Passwörter zu verwalten. Für viele Dienstleistungen muss nur eine Eigenschaft überprüft werden - zum Beispiel das Alter oder der Überziehungsrahmen. In solchen Fällen kann etwa ihre Bank, Ihr Telekommunikationsanbieter oder ihr Arbeitgeber als vertrauenswürdige Stelle fungieren, die dafür garantiert, dass die Eigenschaft zutrifft, ohne ihre Identität preiszugeben.

Verschlüsselung ist eine andere Möglichkeit, Inhalte für andere Personen unleserlich zu machen. Weil alle Formen elektronischer Kommunikation belauscht oder manipuliert werden können, ist es in vielen Fällen entscheidend, dass die Kommunikation in verschlüsselte Form stattfindet.

sogar wenn er in seinem eigenen Wohnzimmer in einem anderen Land sitzt.

Er versucht, sie nicht zu oft zu beobachten - es meint, dass er schon ein wenig zu sehr

in ihr Privatleben eindringt, aber er hat einige Vorgaben programmiert, die Alarme auslösen, etwa wenn sie sich lange Zeit in ihrem Haus nicht bewegt oder wenn sie nachts nicht nachhause kommt. Schließlich wird sie älter, und er kann sich ja nicht so um sie kümmern, wie es eigentlich sein sollte, weil er an einem anderen Land lebt. Sein Telefon läutet: "Hallo, ich bin es, Mama! Ich bin jetzt auf dem Weg zu euch - ich sollte in etwa drei Stunden am Bahnhof ankommen".

- 0 -

Fragebogen zu Sicherheitstechnologien und Privatsphäre

Herzlich willkommen zur Meinungsbefragung über Einstellungen zu Sicherheitstechnologien und Privatsphäre im Rahmen des PRISE-Projekts!

In diesem Fragebogen wird Ihnen eine Serie von Fragen gestellt. *Bitte kreisen Sie die Nummer neben der Antwort ein, die Sie geben wollen.* Sie dürfen nur *eine* Antwort auf jede Frage geben, außer es ist ausdrücklich erwähnt, dass "Sie mehr als eine Antwort auf diese Frage geben können". Falls Sie eine Antwort irrtümlich oder ungewollt einkreisen, streichen Sie diese bitte durch und kreisen dann die richtige Antwort ein. Sie können jederzeit Fragen stellen, wenn Sie beim Ausfüllen nicht sicher sind, wie einzelne Fragen gemeint sind.

Zu Ihrer Person:

1. Geschlecht

1. männlich
2. weiblich

2. Alter

- Alter: ____

3. Wie viele Personen leben in Ihrem Haushalt?

1. 1 Person
2. 2 Personen
3. 3 Personen
4. 4 Personen oder mehr

4. Haben Sie Kinder?

1. Ja
2. Nein

5. Wohnen Kinder bei Ihnen zuhause? (*Mehr als eine Antwort möglich*)

1. Nein
2. Ja, 14 Jahre oder jünger
3. Ja, älter als 14 Jahre

6. Was ist Ihre höchste abgeschlossene Ausbildung?

1. Volks- oder Hauptschulabschluss
2. Realschulabschluss
3. Fachabitur
4. Abitur
5. Lehre oder Ausbildung
6. Fachhochschule oder Universität

7. Welchen Beruf haben Sie?

- Beruf: _____

8. Leben Sie in einer Stadt oder auf dem Land?

1. Großstadt
2. Kleinstadt
3. Ländlicher Bezirk

9. Wie oft verwenden Sie ein Mobiltelefon?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich verwende kein Mobiltelefon

10. Wie oft schreiben Sie E-Mails?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich schreibe nie E-Mails

11. Wie oft verwenden Sie das Internet?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich verwende das Internet nie

12. Wie oft reisen Sie mit öffentlichen Verkehrsmitteln?

1. Mindestens einmal am Tag
2. Mindestens einmal in der Woche
3. Mindestens einmal im Monat
4. Seltener als einmal im Monat
5. Ich reise nie mit öffentlichen Verkehrsmitteln

13. Wie oft reisen Sie mit dem Flugzeug (Hin- und Rückflug zählen als eine Reise)?

1. Mehr als 5mal pro Jahr
2. 3-5mal pro Jahr
3. 1-2mal pro Jahr
4. Seltener als 1 mal pro Jahr
5. Nie

14. Wie oft reisen Sie mit dem Auto?

1. Mindestens einmal am Tag
 2. Mindestens einmal in der Woche
 3. Mindestens einmal im Monat
 4. Seltener als einmal im Monat
 5. Ich reise nie mit dem Auto
-

Allgemeine Fragen zu Sicherheitstechnologien und Privatsphäre

Im Folgenden finden Sie eine Reihe von Ansichten oder Behauptungen über Sicherheitstechnologien und Privatsphäre, die in öffentlichen Debatten oft gebraucht werden. In welchem Ausmaß sind Sie mit diesen Aussagen einverstanden?

Geben Sie bitte für jede Aussage an, inwieweit Sie mit ihr einverstanden sind.

- Wenn Sie glauben, dass die Aussage völlig richtig ist, kreisen Sie bitte 1 "Ich bin völlig einverstanden" ein.
- Wenn Sie glauben, dass die Aussage richtig ist, aber einige Vorbehalte haben, kreisen Sie bitte 2 "Ich bin teilweise einverstanden" ein.
- Wenn Sie es unmöglich finden, zu beurteilen, ob die Aussage richtig oder falsch ist, wählen Sie bitte 3 "Ich bin weder einverstanden noch nicht einverstanden".
- Wenn Sie glauben, dass die Aussage falsch ist, aber einige Zweifel haben, wählen Sie bitte 4 "Ich bin teilweise nicht einverstanden".
- Wenn Sie glauben, dass die Aussage völlig falsch ist, kreisen Sie 5 "Ich bin überhaupt nicht einverstanden" ein.

15. "Die Sicherheit der Gesellschaft hängt völlig von der Entwicklung und Nutzung neuer Sicherheitstechnologien ab".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

16. "Viele Sicherheitstechnologien erhöhen nicht wirklich die Sicherheit, sondern werden nur eingesetzt, um zu zeigen, dass etwas gegen den Terrorismus getan wird".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

17. "Wer nichts zu verbergen hat, muss sich auch nicht vor Sicherheitstechnologien fürchten, die die Privatsphäre verletzen".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden

3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

18. "Wenn Sicherheitstechnologien verfügbar sind, könnten wir sie ohne weiteres auch benutzen".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

19. "Die Privatsphäre sollte nicht ohne einen begründeten Verdacht auf kriminelle Absichten verletzt werden".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

20. "Es ist unangenehm, überwacht zu werden auch wenn man keine kriminellen Absichten hat".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

21. "Neue Sicherheitstechnologien werden wahrscheinlich von staatlichen Behörden missbraucht werden".

1. Ich bin völlig einverstanden

2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

22. "Neue Sicherheitstechnologien werden wahrscheinlich von Verbrechern missbraucht werden".

1. Ich bin völlig einverstanden
 2. Ich bin teilweise einverstanden
 3. Ich bin weder einverstanden noch nicht einverstanden
 4. Ich bin teilweise nicht einverstanden
 5. Ich bin überhaupt nicht einverstanden
-

Sicherheitstechnologien

In diesem Abschnitt möchten wir Sie zu Ihrer Einstellung zu bestimmten Sicherheitstechnologien und ihrer Verwendung befragen.

In den grauen Textboxen finden Sie sehr kurze Beschreibungen der Technologien, die in den anschließenden Fragen diskutiert werden. Mehr Informationen zu diesen Technologien finden Sie in den Szenarien, die an Sie ausgesandt wurden und auch hier ausliegen.

Ein Teil dieser Fragen bezieht sich auf akzeptable Anwendungen dieser Technologien; hier wird es zumeist möglich sein, mehr als eine Antwort zu geben.

Der andere Teil der Fragen betrifft bestimmte Aussagen. Für jede Aussage möchten wir Sie bitten, anzugeben in welchem Ausmaß Sie mit ihr einverstanden sind.

Biometrische Verfahren

Biometrische Verfahren identifizieren Personen automatisch aufgrund ihrer biologischen Merkmale oder ihres Verhaltens. Biometrische Verfahren können verwendet werden, um Zugang zu Gebäuden oder zu Information (Computern, Daten) zu kontrollieren. Die am häufigsten gebrauchten Verfahren nutzen Fingerabdrücke oder Gesichtsmuster.

Biometrische Merkmale können in Form des Originals oder als so genannte „Templates“ gespeichert werden. Das Template ist ein reduzierter digitaler Datensatz, der aus dem Original abgeleitet wird. Aus Datenschutzgründen wird empfohlen, nur das Template zu speichern und das Original zu löschen. Bei Ausweisen und Strafverfolgungsbehörden werden jedoch oft auch die Originalabbildungen aufbewahrt, etwa bei biometrischen Reisepässen oder Gesichtserkennungssystemen.

Einer der wesentlichen Vorteile von biometrischen Verfahren ist, dass ein starker Bezug zur jeweiligen Person vorhanden ist. Biometrische Verfahren ermöglichen bessere Zugangskontrollen und Identitätsdiebstahl wird viel schwieriger, wenn persönliche Daten an die biometrischen Merkmale der Person gebunden sind. Dies ist auch der größte Nachteil biometrischer Systeme. Ist ein Satz von biometrischen Daten einmal geknackt, so ist er für immer verloren.

Biometrischer Reisepass

Ein biometrischer Reisepass besteht aus dem normalen Dokument mit einem zusätzlich eingebetteten Chip, der die biometrischen Daten enthält. Der Chip kann von einem Lesegerät auch aus einem gewissen Abstand gelesen werden.

Biometrische Reisepässe haben Debatten verursacht, weil befürchtet wird, dass die im Chip gespeicherten biometrischen Informationen ohne Wissen des Eigentümers gestohlen werden könnten, indem der Datenaustausch belauscht oder heimlich Lesegeräte in die Nähe gebracht werden.

Eine Herausforderung für biometrische Systeme im Allgemeinen ist es, eine Balance zwischen der False Acceptance Rate (FAR) und False Rejection Rate (FRR) zu finden. Von *falscher Annahme* (oder *falsch positiv*) spricht man, wenn ein System eine Person fälschlicherweise identifiziert. Wenn das System hingegen eine registrierte Person nicht identifiziert, dann spricht man von *falscher Ablehnung* (oder *falsch negativ*).

23. Welche biometrischen Verfahren würden Sie persönlich bei Zugangskontrollen nicht stören? (Mehr als eine Antwort möglich)

1. Gesichtserkennung
2. Fingerabdrücke
3. Iriserkennung

4. Es gibt kein biometrisches Verfahren, das mich bei Zugangskontrollen nicht stören würde
5. Ich weiß es nicht

24. In welchen Fällen ist die Anwendung biometrischer Verfahren für Zugangskontrollen akzeptabel? (Mehr als eine Antwort möglich)

1. Für Sicherheitskontrolle in Banken
2. Für Flughafensicherheit
3. Für Sicherheitskontrollen in Geschäften oder Einkaufszentren
4. Für Grenzkontrollen
5. Für Sicherheitskontrollen in zentralen Bus- und Zugbahnhöfen
6. Für Sicherheitskontrollen in Sportstadien und bei anderen Großereignissen
7. Für Sicherheitskontrollen bei anderen, nicht angeführten privaten Ereignissen oder Dienstleistungen
8. Sie sind nie akzeptabel
9. Ich weiß es nicht

Ausgewählte Aussagen zu biometrischen Verfahren

25. "Biometrische Daten (z.B. Fingerabdrücke oder DNS-Proben) von allen Bürgern in einer zentralen Datenbank zu speichern, ist ein akzeptabler Schritt, um Verbrechen zu bekämpfen".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

26. "Bei der Nutzung biometrischer Reisepässe fühle ich mich wegen des Risikos, dass meine biometrischen Daten gestohlen werden könnten, verunsichert".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Videoüberwachung

Von Videoüberwachung mit *aktiven Kameras* spricht man, wenn die Person, die die Vorgänge am Monitor beobachtet, die Kamera durch Bewegungen oder Zoomen steuern kann, um einer Person oder einer sich abzeichnenden problematischen Situation folgen zu können. Aktive Kameras können mit automatisierten visuellen Überwachungsprogrammen kombiniert werden, die komplizierte Verfahren verwenden, um verdächtiges Verhalten zu erkennen oder Personen anhand von in Datenbanken gespeicherten Fotos zu identifizieren.

Passive Kameras: Diese Kameras zeichnen auf, was in einer bestimmten Stelle (zum Beispiel in einem Kiosk) geschieht. Die Aufzeichnungen werden nur dann betrachtet, wenn es besondere Vorfälle gibt, etwa einen Raub, Kampf usw.

Automatische Gesichtserkennung

Bei automatischen Gesichtserkennungssystemen wird das Gesicht einer Person automatisch erfasst und mit in einer Datenbank gespeicherten Informationen zur Identifikation oder Zugangskontrolle verglichen. Solche Systeme werden normalerweise verwendet, um sicherzustellen, dass eine Person beispielsweise nicht auf einer Liste von bekannten Verbrechern oder Terroristen ist.

Automatische Kennzeichenerfassung

Diese Systeme werten die von Videokameras erfassten Nummerntafeln aus und vergleichen sie mit einer Datenbank. Systeme zur Kennzeichenerkennung werden in mehreren Ländern eingesetzt. Hauptsächlich werden sie verwendet, um Mautvergehen oder Geschwindigkeitsübertretungen zu verfolgen, aber sie werden auch verwendet, um gestohlene Fahrzeuge zu identifizieren.

Personenscanner („Nackte Maschine“)

Röntgen- oder Terrahertzstrahlen können Materialien durchdringen. Sie können daher auch für die Entdeckung und Darstellung von unter der Kleidung verborgenen Gegenständen verwendet werden.

Ein Personenscanner nutzt diese Technik, um zu erkennen, ob eine Person Waffen oder Sprengstoffe an ihrem Körper versteckt hat. Es gibt sehr unterschiedliche Systeme; manche offenbaren alles unter der Kleidung - nicht nur Waffen oder Sprengstoffe - daher stammt auch aus dem Englischen übernommene Name „**Nackte Maschine**“ (naked machine). Diese Art der Sicherheitstechnologie ist am Londoner Flughafen Heathrow (Terminal 4) seit 2004 getestet worden. Andere Systeme nehmen Bilder von verborgenen Objekten auf und projizieren sie auf eine geschlechtslose Puppe.

27. Wo können Sie Videoüberwachung akzeptieren? (Mehr als eine Antwort möglich)

1. In Geschäften
2. In Umkleidekabinen, um Ladendiebstahl zu verhindern
3. In zentralen Bus- und Zugbahnhöfen
4. In Banken
5. In Flughäfen
6. In Sportstadien und bei anderen Großereignissen
7. An allen öffentlichen Orten
8. Sie ist nirgendwo akzeptabel
9. Ich weiß es nicht

28. Was denken Sie über die Anzahl von Überwachungskameras auf öffentlichen Plätzen im Allgemeinen?

1. Es sollte mehr Überwachungskameras auf öffentlichen Plätzen geben
2. Die Anzahl von Überwachungskameras auf öffentlichen Plätzen ist angemessen
3. Es sollte weniger Überwachungskameras auf öffentlichen Plätzen geben
4. Es sollte überhaupt keine Überwachungskameras auf öffentlichen Plätzen geben
5. Ich weiß es nicht

29. In welchen Fällen ist das Scannen von Personen nach versteckten Gegenständen notwendig? (Mehr als eine Antwort möglich)

1. In Schulen
2. In zentralen Bus- und Zugbahnhöfen
3. In Flughäfen
4. In Einkaufszentren
5. Es ist nie notwendig
6. Ich weiß es nicht

30. Welche Art des Scannens würden Sie akzeptabel finden? (Mehr als eine Antwort möglich)

1. Ein Scannen, das alles unter der Kleidung zeigt
2. Eine Durchleuchtung, bei der versteckte Gegenstände auf eine Puppe projiziert werden
3. Die Messung von Körperhitze, Schweiß und Pulsfrequenz
4. Das Scannen nach metallischen Gegenständen
5. Eine Durchleuchtung des Gepäcks mittels Röntgenstrahlen
6. Das Scannen ist nie akzeptabel
7. Ich weiß es nicht

Ausgewählte Aussagen zu Videoüberwachung und dem Scannen von Personen

31. "Durch Videoüberwachung fühle ich mich sicherer"

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

32. "Videoüberwachung verletzt meine Privatsphäre"

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

33. "Das Scannen von Personen nach versteckten Gegenständen ist ein akzeptables Mittel, um Terrorismus zu verhindern"

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Technologien zur Ortung

Es ist möglich, die ungefähre Position von Mobiltelefonen aus den Koordinaten der nächstgelegenen Funkstationen zu berechnen.

Für eine genauere Ortung werden satellitenbasierte Systeme genutzt:

GPS ist das derzeit vorhandene System, die Abkürzung steht für *Global Positioning System*. Das zukünftige System heißt *Galileo* und soll im Jahr 2010 betriebsbereit sein. Es wird genauer als das GPS-System sein, und soll auch innerhalb von Gebäuden funktionieren.

eCall

Das eCall-System soll in Autos eingesetzt werden. Das Gerät enthält Sensoren, die es nach einem Unfall aktivieren. Es löst einen automatischen Notruf aus und übermittelt Information über die Zeit, den genauen Standort und das betroffene Fahrzeug.

Das Gerät wird nicht permanent mit einem mobilen Datenübertragungsnetz verbunden sein, es verbindet sich nur, nachdem es aktiviert worden ist. Es gibt jedoch Befürchtungen, dass sich dies ändern könnte: ein Beispiel wäre das permanente Senden von weiteren Daten, etwa für Versicherungsgesellschaften. Sorgen bereitet auch ein möglicher unbefugter Zugang zu Datenbanken, in denen eCall-Daten gespeichert werden. Ab September 2009 werden alle neuen Autos in den teilnehmenden Ländern mit eCall-Geräten ausgerüstet sein.

34. Für welchen Zweck ist die Ortung von Mobiltelefonen akzeptabel? (Mehr als eine Antwort möglich)

1. Polizeiliche Ortung der Mobiltelefone von vermuteten Terroristen oder Verbrechern aufgrund einer gerichtlichen Anordnung
2. Polizeiliche Ortung jedes Mobiltelefons ohne gerichtliche Anordnung
3. In Notfällen, z.B. bei einem Unfall, einem verlorenen Kind oder einer verwirrten Person
4. Sie ist nie akzeptabel
5. Ich weiß es nicht

35. Für welchen Zweck ist die Ortung von Autos akzeptabel? (Mehr als eine Antwort möglich)

1. Polizeiliche Ortung der Autos von vermuteten Terroristen oder Verbrechern aufgrund einer gerichtlichen Anordnung
2. Polizeiliche Ortung jedes Autos ohne gerichtliche Anordnung
3. Ortung um gestohlene Fahrzeuge ausfindig zu machen
4. Um Geschwindigkeitskontrollen durchzuführen und Strafmandate auszustellen
5. Automatischer Notruf im Falle eines Autounfalls
6. Sie ist nie akzeptabel
7. Ich weiß es nicht

36. Sollte das eCall-System automatisch in allen neuen Autos installiert werden?

1. Ja
2. Ja, aber es sollte möglich sein, eCall auszuschalten
3. Nein, es sollte eine Wahlmöglichkeit geben
4. Nein, es sollte keinesfalls installiert werden
5. Ich weiß es nicht

Ausgewählte Aussagen zu Ortungstechnologien**37. "Die Möglichkeit, alle Mobiltelefone zu orten, verletzt die Privatsphäre".**

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

38. "Die Möglichkeit, die Mobiltelefone von Verdächtigen orten zu können, ist ein gutes Werkzeug für die Polizei bei der Untersuchung von und Vorbeugung gegen Terrorismus und Kriminalität".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

39. "Die Möglichkeit, alle Autos orten zu können, verletzt die Privatsphäre".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

40. "Die Möglichkeit, alle Autos orten zu können, ist ein gutes Werkzeug für die Polizei bei der Untersuchung von und Vorbeugung gegen Terrorismus und Kriminalität".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Vorratsdatenspeicherung

Eine Datenbank ist eine organisierte Sammlung von Daten. Es wird allgemein anerkannt, dass man wesentlich mehr über eine Person erfahren kann, wenn Daten aus verschiedenen Quellen zusammengefügt werden als wenn diese Daten jeweils einzelnen betrachtet werden. Es ist daher ein wichtiges Prinzip des Datenschutzes, dass in Datenbanken jeweils nur jene Informationen gesammelt werden dürfen, die für den Zweck dieser Datenbank notwendig sind, und dass die Daten gelöscht werden sollen, sobald sie nicht mehr benötigt werden.

In letzter Zeit ist ein Trend zu beobachten, nach dem Regierungen mehr Daten als für den ursprünglichen Zweck erforderlich sind, speichern wollen und unterschiedliche Datenbanksysteme für Zwecke wie Sicherheit zusammenführen wollen. Zumeist sind Daten aus dem Bereich Informations- und Kommunikationstechnologien, wie Kommunikationsverkehrsdaten von Telefonen, Mobiltelefonen und Internetnutzung gemeint, wenn die Einführung von Vorratsdatenspeicherung diskutiert werden.

Total Information Awareness (TIA)

TIA war ein Programm der DARPA (Defence Advanced Research Projects Agency) der US-Regierung. Es lässt sich am ehesten mit dem Begriff "allumfassende Auswertung von Informationen" übersetzen. Das TIA-Programm umfasste drei Kategorien von Software-Werkzeugen: automatische Sprachübersetzung, Suchmaschinen und Mustererkennung sowie fortgeschrittene sowie fortgeschrittene Systeme zur Entscheidungsfindung.

Das Ziel von TIA war es, terroristische Angriffe vorhersagen zu können, ehe sie eintreten. Es war beabsichtigt, dass das System private und öffentliche Datenbanken wie auch das Internet nach verdächtigen Daten durchsucht, die auf einen Terroristenangriff hinweisen könnten. Im September 2003 wurde die Finanzierung von TIA vom US-Kongress gestoppt, aber viele der Projekte innerhalb des Programms werden unter anderem Namen weitergeführt.

Zweckentfremdung

Datenbanksysteme sind gegenüber Zweckentfremdungen anfällig, darunter versteht man die Verwendung von Daten für andere Aufgaben als ursprünglich geplant. Ein Beispiel dafür ist die norwegische Datenbank über Asylanttragsteller, die auch biometrische Informationen wie Fingerabdrücke enthält. Sie wurde der Polizei für Ermittlungen von strafbaren Handlungen zur Verfügung gestellt. Der ursprüngliche Zweck der Datenbank war es, die Identität von Asylanten zu überprüfen.

41. Für welche der folgenden Zwecke finden Sie Vorratsdatenspeicherung von Kommunikationsverkehrsdaten akzeptabel? (Mehr als eine Antwort möglich)

1. Zur Verhütung von terroristischen Angriffen im Allgemeinen
2. Für die Untersuchung von terroristischen Angriffen
3. Zur Verhütung von Verbrechen im Allgemeinen
4. Für die Untersuchung von Verbrechen
5. Für kommerzielle Zwecke
6. Sie ist nie akzeptabel
7. Ich weiß es nicht

42. Für welche der folgenden Zwecke finden Sie die Verknüpfung und Auswertung von persönlichen Daten aus verschiedenen Datenbanken akzeptabel? (Mehr als eine Antwort möglich)

1. Zur Verhütung von terroristischen Angriffen im Allgemeinen
2. Für die Untersuchung von terroristischen Angriffen
3. Zur Verhütung von Verbrechen im Allgemeinen
4. Für die Untersuchung von stattgefundenen Verbrechen
5. Für kommerzielle Zwecke
6. Es ist nie akzeptabel

7. Ich weiß es nicht

Ausgewählte Aussagen zur Vorratsdatenspeicherung

43. "Öffentliche Stellen sollten alle Daten speichern, die sie aus Sicherheitsgründen als notwendig betrachten".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

44. "Daten von Telefon, Mobiltelefon und Internetnutzung sollten nicht über das Ausmaß hinaus gespeichert werden, welches für Abrechnungszwecke erforderlich ist".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

45. "Die Auswertung und Verknüpfung von Daten aus unterschiedlichen Datenbanken mit persönlichen Informationen verletzt die Privatsphäre".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

46. "Die Auswertung und Verknüpfung von Daten aus unterschiedlichen Datenbanken, ist ein gutes Werkzeug für die Polizei, um Terrorismus zu verhindern".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

47. "Dass Datenbanken für etwas anderes als den Originalzweck verwendet werden, ist ein ernstes Problem für die Privatsphäre".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Abhören

Unterschiedliche Technologien können genutzt werden, um die Aktivitäten und Kommunikation von Bürgern im Internet, beim Telefonieren oder in bestimmten Gebieten zu belauschen. Eine bekannte Form ist das Abhören von Telefongesprächen. Dabei wird ein Abhörgerät in Telefonzentralen installiert, das Abhörgerät kann die Gespräche des Verdächtigen erfassen oder auch gegen Telefone von Personen gerichtet werden, von denen man annimmt, dass der Verdächtige sich an sie wenden wird.

Eine erweiterte Version des Abhörens erfasst unterschiedslos alle Kommunikationsmöglichkeiten (Telefon, Mobiltelefon, Internet), die auf verdächtige Aktivitäten untersucht werden.

48. Für welche der folgenden Zwecke ist das Abhören akzeptabel? (Mehr als eine Antwort möglich)

1. Zur Verhütung und Untersuchung von terroristischen Angriffen aufgrund einer gerichtlichen Anordnung
2. Zur Verhütung und Untersuchung von terroristischen Angriffen ohne gerichtliche Anordnung
3. Zur Verhütung und Untersuchung von Verbrechen aufgrund einer gerichtlichen Anordnung
4. Zur Verhütung und Untersuchung von Verbrechen ohne gerichtliche Anordnung
5. Für kommerzielle Zwecke

6. Es ist nie akzeptabel
7. Ich weiß es nicht

49. Welche Methoden des Abhörens von Telefongesprächen durch die Polizei sind akzeptabel?

1. Das Abhören aller Gespräche auf mögliche Hinweise
2. Das Abhören von Verdächtigen und Personen, die diese möglicherweise kontaktieren werden
3. Das Abhören von Verdächtigen
4. Das Abhören ist völlig unannehmbar
5. Ich weiß es nicht

Ausgewählte Aussagen zum Abhören

50. "Abhören ist ein gutes Werkzeug für polizeiliche Ermittlungen".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

51. "Abhören ist eine ernste Verletzung der Privatsphäre".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

Technologien zur Förderung der Privatsphäre
Technologien, die direkt dazu beitragen, die Privatsphäre zu schützen, werden als privatsphärenfördernde oder privatsphärenfreundliche Technologien bezeichnet.

Anonymisierung ist ein Beispiel dafür. Es gibt Dienste, die eine anonyme elektronische Kommunikation für normale Benutzer ermöglichen. Dabei werden die Verbindungen zwischen Nutzen und die Spuren, die sie hinterlassen versteckt.

Identitäts-Management ist auch eine Form privatsphärenfördernder Technologien: In einigen Fällen wollen Sie sich vielleicht nicht identifizieren, sondern ein Pseudonym (zum Beispiel bei Foren im Internet) verwenden. Um die Verknüpfung von Daten schwieriger zu machen, kann es nützlich sein, verschiedene Benutzernamen (die Ihre Identität nicht zeigen) und Passwörter für verschiedene Zwecke zu verwenden. Identitätsmanagementsysteme helfen Ihnen dabei, Ihre verschiedenen Benutzernamen und Passwörter zu verwalten.

Verschlüsselung ist eine andere Möglichkeit, Inhalte für andere Personen unleserlich zu machen. Weil alle Formen elektronischer Kommunikation belauscht oder manipuliert werden können, ist es in vielen Fällen entscheidend, dass die Kommunikation in verschlüsselte Form stattfindet.

52. Welche Arten von privatsphärenfördernden Technologien sollten legaler Weise für alle Bürger verfügbar sein? (Mehr als eine Antwort möglich)

1. Anonyme Telefon-Guthaben Karten
2. Verschlüsselungssoftware
3. Identitätsmanagementsysteme
4. Keine privatsphärenfördernden Technologien sollten legal verfügbar sein
5. Ich weiß es nicht

Ausgewählte Aussagen zu privatsphärenfördernden Technologien

53. "Privatsphärenfördernde Technologien sind in der Gesellschaft von heute eine Notwendigkeit, um die Privatsphäre zu erhalten".

1. Ich bin völlig einverstanden
2. Ich bin teilweise einverstanden
3. Ich bin weder einverstanden noch nicht einverstanden
4. Ich bin teilweise nicht einverstanden
5. Ich bin überhaupt nicht einverstanden

54. " Privatsphärenfördernde Technologien sollten nicht legal sein, wenn sie polizeiliche Ermittlungen und die Verhütung von Terrorismus und Verbrechen schwieriger machen".

1. Ich bin völlig einverstanden
 2. Ich bin teilweise einverstanden
 3. Ich bin weder einverstanden noch nicht einverstanden
 4. Ich bin teilweise nicht einverstanden
 5. Ich bin überhaupt nicht einverstanden
-

Dilemmas in der Verwendung der Sicherheitstechnik

Im Folgenden stellen wir Ihnen jetzt eine Reihe von Dilemmas vor, die bei der Nutzung von Sicherheitstechnologien für die Privatsphäre auftreten. Wir möchten Sie bitten, dass Sie für jede Frage sowohl über Vorteile als auch Nachteile nachdenken und dann Ihre Antwort geben. *Auf alle Fragen in diesem Abschnitt können Sie mehr als eine Antwort geben.*

55. Die Nutzung von Fingerabdrücken beim Ein- und Aussteigen in öffentliche Verkehrsmittel könnte eine automatische Abbuchung der Fahrtkosten von Ihrem Konto ermöglichen. Dies würde die Bezahlung um einiges leichter machen, würde aber bedeuten, dass Ihre Fahrten gespeichert werden und Sie ihre Fingerabdrücke als Ausweis benutzen müssen. Wie würden Sie sich dabei fühlen? (Mehr als eine Antwort möglich)

1. Ich kann die Speicherung meiner Fahrten und die Nutzung von Fingerabdrücken akzeptieren, weil dadurch die Bezahlung einfacher wird.
2. Ich kann dies nur akzeptieren, wenn meine Fingerabdrücke nur als „Templates“ gespeichert sind und diese nicht rekonstruiert werden können.
3. Ich kann dies nur akzeptieren, wenn die Daten zu meinen gespeicherten Reisen nach der Bezahlung gelöscht werden.
4. Die Verwendung von Fingerabdrücken zu verwenden, sollte eine Möglichkeit, aber nicht die einzig verfügbare Form der Bezahlung sein.
5. Ich würde meine Fingerabdrücke nie als Identifikation bei der Nutzung öffentlicher Verkehrsmittel verwenden.
6. Ich weiß es nicht.

56. Eine umfassende Registrierung in einer Flughafendatenbank und die Akzeptanz von bestimmten Sicherheitstechnologien, die alle als verletzend für die Privatsphäre angesehen werden können, würden eine schnelle Abfertigung in Flughäfen ermöglichen. Welche Sicherheitstechnologien und Verletzungen ihrer Privatsphäre würden Sie für eine schnellere Abfertigung im Flughafen akzeptieren? (Mehr als eine Antwort möglich)

1. Ich würde es akzeptieren, umfassend überprüft und in einer permanenten Flughafensicherheitsdatenbank gespeichert zu werden und dann bei allen weiteren Flügen biometrische Verfahren zur Identifizierung zu verwenden.
2. Ich würde es akzeptieren, durch "nackte Maschinen" zu gehen.
3. Ich würde es akzeptieren, dass Schweiß, Körpertemperatur und Pulsfrequenz gemessen werden.
4. Ich würde meine Privatsphäre nicht für ein schnelles und bequemes Check-In am Flughafen aufgeben.
5. Ich weiß es nicht.

57. Aktive Überwachungskameras und automatische Gesichtserkennung, bei der Gesichter von Menschen mit den in einer Datenbank gespeicherten Fotografien von bekanntem Terroristen abgeglichen werden, sind Sicherheitstechnologien, die verwendet werden können, um Terrorangriffe z.B. in Flughäfen oder Bahnhöfen zu verhindern. Diese Sicherheitstechnologien könnten möglicherweise einen Terrorangriff verhindern, aber ihre Wirksamkeit ist nicht bewiesen. Sie könnten auch dazu führen, dass unschuldige Personen mit Terroristen verwechselt und ausführlichen Befragungen unterzogen werden. Unter welchen Bedingungen sollen diese Technologien eingesetzt werden? (Mehr als eine Antwort möglich)

1. Aktive Kameras und automatische Gesichtserkennung sollten eingesetzt werden, ganz gleich wie viele unschuldige Personen mit Terroristen verwechselt werden.
2. Aktive Kameras und automatische Gesichtserkennung sollten eingesetzt werden, aber nur wenn wenige unschuldige Personen mit Terroristen verwechselt werden.
3. Aktive Kameras und automatische Gesichtserkennung sollten nur eingesetzt werden, wenn niemand mit Terroristen verwechselt wird.
4. Aktive Kameras und automatische Gesichtserkennung sollten nur an Orten eingesetzt werden, an denen viele Verbrechen aufgetreten sind oder die sehr verwundbar für Terrorangriffe sind.
5. Aktive Kameras und automatische Gesichtserkennung sollten nirgendwo benutzt werden.
6. Ich weiß es nicht.

58. Neue Technologien machen es möglich, Daten von verschiedenen Datenbanken, welche persönliche Informationen beinhalten, zu verknüpfen und zu durchsuchen, um verdächtige Muster in der persönlichen Kommunikation und Internetnutzung zu entdecken. Der Zweck ist, Angriffe vorzusehen und zu verhindern, aber dies bedeutet auch, persönliche Daten von unschuldigen Personen zu analysieren. Welche Möglichkeiten für die Polizei zur Verknüpfung der Durchsuchung verschiedener Datenbanken finden Sie akzeptabel? (Mehr als eine Antwort möglich)

1. Die Polizei sollte Zugriff auf alle Datenbanken haben und sie kombinieren können, um verdächtige Muster zu finden, die mögliche Terroristen identifizieren können.
2. Die Polizei sollte nur Zugriff auf Datenbanken haben und sie kombinieren können, wenn die Daten anonym sind und nur durch einen Gerichtsbeschluss die Identität eines Verdächtigen offen gelegt werden darf.
3. Die Polizei sollte niemals Datenbanken kombinieren nach verdächtigen Muster durchsuchen dürfen.
4. Ich weiß es nicht.

59. Das eCall-System könnte in allen neuen Autos installiert werden, um im Falle eines Unfalls einen Notruf auszusenden. Dieses System könnte auch verwendet werden, um Autos für andere Zwecke zu orten, z.B. wenn sie gestohlen werden oder wenn sie für Verbrechen oder Terroranschläge verwendet werden. Dies erfordert aber, dass die Bewegungen von Autos mit eCall fortlaufend erfasst und gespeichert werden. Welche Nutzungen von eCall finden Sie akzeptabel? (Mehr als eine Antwort möglich)

1. Ich finde es akzeptabel, dass eCall von der Polizei aktiviert werden kann, um ein Auto ausfindig zu machen, falls es notwendig ist, um Verbrechen oder Terror zu verhindern.
2. Ich finde es akzeptabel, dass eCall jederzeit aktiv ist und benutzt werden kann, um Geschwindigkeitsübertretungen zu bestrafen.
3. Ich finde es akzeptabel, dass die Bewegungen meines Autos mit eCall fortlaufend erfasst und gespeichert werden.
4. eCall sollte nicht für andere Zwecke verwendet werden, als Unfälle zu melden.
5. Das Installieren von eCall Autos sollte freiwillig sein.
6. Ich weiß es nicht.

60. Privatsphärenfördernde Technologien können dazu beitragen, die Privatsphäre zu schützen, wenn man per Telefon oder E-Mail kommuniziert und wenn man das Internet verwendet. Sie können aber auch für strafbare Aktivitäten oder von Terroristen benutzt werden. Wenn es darum geht, die Privatsphäre gewöhnlicher Bürger zu bewahren, welche Risiken sind Sie bereit, für einen legalen Zugang zu privatsphärenfördernden Technologien zu akzeptieren? (Mehr als eine Antwort möglich)

1. Ich kann legale anonyme Telefonguthabekarten akzeptieren, obwohl sie polizeiliche Untersuchungen oder die Verhinderung von Terror und Verbrechen schwieriger machen könnten.
2. Ich kann die legale Verwendung von Verschlüsselungstechnologien akzeptieren, obwohl sie polizeiliche Untersuchungen oder die Verhinderung von Terror und Verbrechen schwieriger machen könnten.
3. Ich kann Anonymität im Internet akzeptieren, selbst wenn es bedeutet, dass Personen, die nach Bombenbauanleitungen suchen, nicht von der Polizei verfolgt werden können.
4. Ich kann akzeptieren, dass Internetanonymität bedeutet, dass Personen, die nach Kinderpornographie suchen, nicht von der Polizei verfolgt werden können.
5. Ich kann keine privatsphärenfördernden Technologien akzeptieren, die polizeiliche Untersuchungen oder die Verhinderung von Terror und Verbrechen schwieriger machen könnten.
6. Ich weiß es nicht.

61. Wenn eine Sicherheitstechnologie einen hohen Grad an Sicherheit bietet, welche Folgen können

Sie für Personen akzeptieren, die diese Technologie nicht nutzen können, und welche für Personen, die sie aus Gründen der Privatsphäre nicht verwenden wollen? (Mehr als eine Antwort möglich)

1. Ich kann es akzeptieren, dass Leute, die aus Gründen der Privatsphäre nicht bereit sind, diese Technologien zu verwenden, von der Nutzung einiger öffentlicher Dienste ausgeschlossen sind.
 2. Ich kann akzeptieren, dass Leute, die außerstande sind, die Technik zu verwenden, davon ausgeschlossen sind, einige öffentliche Dienste zu nutzen.
 3. Ich kann akzeptieren, dass Leute, die aus Gründen der Privatsphäre nicht bereit sind, diese Technologien zu verwenden, in gewisser Weise behindert werden, wenn sie mit öffentlichen Verkehrsmitteln reisen.
 4. Ich kann akzeptieren, dass Leute, die außerstande sind, diese Technologien zu verwenden, in gewisser Weise behindert werden, wenn sie mit öffentlichen Verkehrsmitteln reisen.
 5. Ich kann keinerlei Folgen für Personen akzeptieren, die aus Gründen der Privatsphäre nicht bereit sind, diese Technologien zu verwenden.
 6. Ich kann keinerlei Folgen für Personen akzeptieren, die außerstande sind, diese Technologien zu verwenden.
 7. Ich weiß es nicht.
-

Demokratiepolitische Aspekte

Im folgenden Abschnitt werden Sie mit einigen Aussagen über demokratische Aspekte neuer Sicherheitstechnologien konfrontiert. Wer sollte einen Einfluss bei Fragen von Sicherheitstechnologien und Privatsphäre ausüben dürfen und in welcher Weise?

In welchem Ausmaß sind Sie mit den folgenden Ansichten einverstanden oder stimmen Sie nicht überein? Bitte teilen Sie uns Ihre Meinung zu den einzelnen Ansichten mit. Bitte geben Sie nur eine Antwort auf jede Frage.

62. "Politiker müssen wichtige Fragen immer in öffentlichen Debatten und öffentlichen Anhörungen diskutieren, bevor sie Entscheidungen über die Einführung neuer Sicherheitstechnologien treffen".

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

63. "Das Thema Sicherheit und Privatsphäre ist so kompliziert, dass es keinen Sinn macht, die Öffentlichkeit in Diskussionen dieser Angelegenheit einzubeziehen".

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

64. "Menschenrechtsorganisationen sind immer berechtigt, gehört zu werden, wenn wichtige Entscheidungen über Sicherheit und Privatsphäre getroffen werden".

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

65. "Es ist wichtig, dass private Unternehmen, die an der Herstellung von Sicherheitstechnologien beteiligt sind, auch berechtigt sind, gehört zu werden, wenn wichtige Entscheidungen über Sicherheit und Privatsphäre getroffen werden".

1. Ich bin völlig einverstanden
2. Ich bin teils einverstanden
3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
4. Ich bin teils nicht einverstanden
5. Ich bin nicht einverstanden

66. "Bei bedeutsamen Entscheidungen über die Verwendung von Sicherheitstechnologien ist es unbedingt notwendig, dass alternative Lösungen untersucht und in die Debatte einbezogen werden".

1. Ich bin völlig einverstanden
 2. Ich bin teils einverstanden
 3. Ich bin einverstanden oder bin nicht einverstanden auch nicht
 4. Ich bin teils nicht einverstanden
 5. Ich bin nicht einverstanden
-

Vorschläge zu einer privatsphärenfördernden Verwendung von Sicherheitstechnologien

Im folgenden Abschnitt möchten wir Ihnen einige Vorschläge vorstellen, wie man Sicherheitstechnologien einführen, nutzen und entwickeln kann, ohne die Privatsphäre zu verletzen. Für jeden Vorschlag bitten wir Sie darum, anzugeben, wie wichtig es wäre, den Vorschlag durchzuführen.

Wenn Sie es sehr wichtig finden, dass dem Vorschlag gefolgt wird, kreisen Sie bitte 1 "sehr wichtig" ein.

Wenn Sie den Vorschlag wichtig finden, ihm aber keine hohe Priorität beimessen, wählen Sie 2 "wichtig".

Wenn Sie finden, dass es nicht sehr wichtig ist, wählen Sie 3 "wenig wichtig".

Wenn Sie finden, dass es überhaupt nicht wichtig ist oder dem Vorschlag nicht gefolgt werden sollte, kreisen Sie 4 "überhaupt nicht wichtig" ein.

Wenn Sie nicht sicher sind, was Sie antworten sollen, wählen Sie bitte 5 "Ich weiß es nicht".

Vorschläge

67. Die Sammlung von persönlichen Daten von unverdächtigen Personen muss anonym sein, bis eine Identifikation durch einen Gerichtsbeschluss gestattet wird.

1. Sehr wichtig
2. Wichtig
3. Wenig wichtig
4. Überhaupt nicht wichtig
5. Ich weiß es nicht

68. Nur bevollmächtigtes Personal darf Zugang zu gesammelten persönlichen Daten haben.

1. Sehr wichtig
2. Wichtig
3. Wenig wichtig
4. Überhaupt nicht wichtig
5. Ich weiß es nicht

69. Vor der Einführung müssen neue Sicherheitstechniken auf ihre Wirkungen auf die Privatsphäre hin untersucht werden.

1. Sehr wichtig

2. Wichtig
3. Wenig wichtig
4. Überhaupt nicht wichtig
5. Ich weiß es nicht

70. Die Finanzierung von Forschungsprojekten über neue Sicherheitstechnologien sollte von einer gründlichen Analyse von den Wirkungen auf die Privatsphäre abhängig sein.

1. Sehr wichtig
 2. Wichtig
 3. Wenig wichtig
 4. Überhaupt nicht wichtig
 5. Ich weiß es nicht
-

Abschließende Fragen

Sie haben viele unterschiedliche und detaillierte Fragen über Sicherheitstechniken und Privatsphäre beantwortet. Abschließend möchten wir Ihnen noch zwei Fragen stellen.

72. Haben Sie Ihre Einstellung zu Sicherheitstechnologien im Allgemeinen geändert, während Sie diesen Fragebogen ausgefüllt haben?

1. Ja, meine Einstellung zu Sicherheitstechnologien im Allgemeinen ist positiver geworden
2. Ja, meine Einstellung zu Sicherheitstechnologien im Allgemeinen ist negativer geworden
3. Nein, ich habe meine Einstellung nicht geändert
4. Ich weiß es nicht

73. Wenn Sie weitere Anmerkungen zu Sicherheitstechnologien hinzufügen möchten, oder wenn Sie Kommentare geben möchten, für die in diesem Fragebogen keine Gelegenheit vorgesehen war, so können Sie diese hier hinzufügen:

1. Ich habe nichts hinzuzufügen
2. Ihre Bemerkungen:

Annex 4 - Questionnaire

Annex 5 - Transcript of group interviews

Group 1

Es geht darum, durch den Fragebogen Vergleichbarkeit herzustellen. Das heißt, dass in ganz Europa die gleichen Fragen gestellt wurden. Ein Teil dieser Studie ist abgestimmt darauf, über diese 70 Fragen ein gleiches Meinungsbild zu erheben. Sachen, die in dem Fragebogen zu kurz gekommen sind oder die Ihnen beim Ausfüllen des Fragebogens in den Sinn gekommen sind, sollen jetzt besprochen werden. Ich habe eine Reihe von Fragen, die ich Ihnen stellen möchte. Es geht ungezwungen zu, das heißt, dass Sie sich nicht zu Wort melden, sondern einfach mit dem Reden anfangen dürfen. Meine erste Frage wäre, was ist Ihr erster Gedanke, wenn Sie über sich als Betroffenen von Sicherheitstechnologien und an die Privatsphäre denken. Die einleitenden Worte haben schon Anknüpfungspunkte gegeben oder auch das Ausfüllen des Fragebogens. Was kommt Ihnen in den Sinn, wenn Sie an diese Frage denken?

Also ich glaub dann immer, dass es ziemlich schwierig ist. Gerade, wenn ich mir vorstelle durch solch eine Naked Machine zu gehen oder so. Bis zu einem gewissen Grad ist das ja noch ok. Also, wenn jetzt mein Körper auf so eine Puppe abgebildet wird, da würde ich noch ok sagen, aber wenn es dann wirklich so krass wird und mein ganzer Körper entblößt wird, ok, dahinter stehen ja auch nur Menschen, die sich das angucken. Und ob das mal zu irgendwelchen Zwecken missbraucht wird durch irgendwelche Kerle, die dann sagen: Hey, die sieht doch scharf aus lass die mal dadurch laufen. Ja, das würde mir halt so ein bisschen Angst machen.

Es ist dann sozusagen schwer, eine Balance zu finden. Die Technologie dient sicherlich einem sinnvollen Zweck, aber manchmal ist man mir der Art und Weise, wie sie einen dann betreffen vielleicht nicht mehr einverstanden.

Ja, genau.

Die Technologien, die wir in den Szenarien oder auch in den Fragebögen dargestellt haben, haben Sie da irgendwelche eigenen Erfahrungen oder Anmerkungen dazu? Was ist da Ihre erste Reaktion?

Also, ich habe immer so ein bisschen Angst vor diesen riesigen Datenbanken von denen immer gesprochen wird. Und ich das Gefühl habe, dass alles, was jemals über mich gesammelt wurde jetzt irgendwie europaweit zusammengeführt wird und somit beliebige Leute Anfragen stellen können und allein durch diese Masse der Daten...Es geht ja schon damit los, dass irgendwann mal meine Personalien aufgenommen wurden. Ich bin das letzte Mal durch Kiel gegangen und ging an einem brennenden Mülleimer vorbei und dann kam da die Polizei, die schon gerufen worden war. Und da wurden dann meine Personalien aufgenommen. Und wenn ich dann jetzt ins Fußballstadion will und da denkt sich irgendeiner, gucken wir doch mal, was der so macht und dann steht da irgendwie Brandstiftung, Personalien aufgenommen. Es ist ja auch diese Anonymisierung, vielleicht sehen sie ja auch nur Treffer Brandstiftung. Das kann ja auch in die falsche Richtung gehen. Da habe ich dann Angst, dass ich einmal ins völlig

unvorhergesehen in ein Raster passe, was sich irgendjemand ausgedacht hat. Diese Anonymisierung macht es ja nicht leichter. Für mich ist das ein schwieriger Grad, wenn man nur Treffer sagt und keine Möglichkeit hat diese Treffer zu bewerten und man gerade dafür diese richterliche Anordnung bräuchte. Zum anderen ist es mir unheimlich, dass sehr viele Daten auf sehr vielen Datenbanken irgendwie zusammengeführt werden. Ich nehme immer das Beispiel Telefonbuch, denn da ist irgendwie nie eine einheitliche Form der Daten gegeben, also Name und Straße, das steht immer durcheinander und man weiß gar nicht, was Vor- und Nachname ist und wenn da irgendwas wild zusammengewürfelt wird, dann kann es doch passieren, dass ich dann mit einer anderen Person verwechselt werde. Und beide dann zusammen ein Raster bilden, was mich dann zu einen Terroristen macht.

Ich kann verstehen, dass die Art und Weise, wie Datenbanken mit den Daten umgehen, Sie allgemein beunruhigen.

Ja, ich meine, dass man so etwas ja nicht weiß. Es werden ja auch oft Personalien kontrolliert oder heutzutage, wenn ich ins Stadion gehen will, muss ich ja schon meine Personalien angeben. Wenn ich dann irgendwie in zwei Stadien war, wo es Randalen gegeben hat, dann sagt irgendein System ganz schnell, dass man den mal besser beobachten sollte. Es schwimmt ja auch, wenn diese Systeme selbst machen, was sie wollen. Und wenn man das denn an einer Stelle löscht, dann ist es woanders wahrscheinlich noch drinnen, weil man nicht daran gedacht hat, es überall zu löschen. Und es geht auch darum, wenn da 10 Datenbanken mit Millionen von Datensätzen, wahrscheinlich sogar Milliarden sind, bekommt man die auch nicht richtig gepflegt.

Das Stimmt. Das ist ein grundsätzliches Problem, dass nicht überall, wo Daten ...verfügbar sind, Sie das wissen können. Und unter Umständen, wenn Daten nicht mehr vorgehalten werden können, kann eine Löschung durchgeführt werden. Es gibt zum Beispiel im Bereich Fußballstadion eine sogenannte Gewalttäterdatei Sport von Hooligans, die dann der Polizei bekannt sind, das heißt, dass Sie da durch eine einfache Überprüfung in das Stadium nicht rein. Es sollen aber diejenigen, die in dieser Datenbank sind, durch die Ausweisüberprüfung draußen behalten werden. Das ist also der Hintergrund.

Da habe ich dann noch mal zur WM ein Beispiel gehört, dass die irgendwie Leute, deren Personalien im Zusammenhang mit solchen Eskalationen aufgenommen wurden, dazu verpflichtet haben sich vor und nach den Spielen bei der Polizei zu melden. Das fand ich doch etwas vage, muss ich sagen.

Dass Sie sich polizeilich melden müssen, ist eine Tendenz, die wir bei solchen Großveranstaltungen haben, weil dort eine große Menschenmenge ist und das Problem besteht, dass es nicht leicht zu lokalisieren ist, wer gefährlich ist oder von wem eine Gefahr ausgehen kann.

Ich habe die Vermutung, dass es allgemein so ist, dass sich alle auf die Präventionen stürzen. Wir lassen mal den Computer nach irgendwelchen Kriterien, die wir nicht kennen und sich irgendjemand nur ausgedacht hat gucken. Wer könnte mir denn gefährlich sein? Da hängen wir uns dann mal dran.

Das ist ja noch nicht alles. Nicht nur die Frage „Wer könnte gefährlich sein?“, sondern auch eine bestimmte Besonderheit, die auf einen bestimmten Moment draufpasst. Immer wenn das Thema Terrorismus kommt, gehen mir die Haare hoch, weil man ja nicht immer wenn es eine

neue Datenbank gibt einfach mal gucken kann, ob es dort wieder einen neuen Anhaltspunkt gibt, den man überprüfen sollte. Das ist ein Syndrom, womit gerechtfertigt wird, dass die gesamte Bevölkerung latent kriminalisiert wird. Es könnte ja einer dabei sein und das finde ich nicht gut. Jedes mal, wenn ein neuer Innenminister kommt, fängt der ganz normal an und nach einem halben Jahr will er immer andere Gesetze haben. Ich weiß nicht, ob die irgendwelche Daten haben, die wir nicht haben. Für mich ist das einfach nicht nachvollziehbar.

Die Rasterfahndung wurde wegen des RAF-Terrorismus eingeführt. Damals war es einfacher die Rasterung auf einen vorher bekannten Personenkreis einzugrenzen. Man wusste, dass RAF-Terroristen sich keine Konten besorgen und man suchte nach Personen, die ihre Gasrechnungen bar bezahlten und man meinte damit RAF-Terroristen eingrenzen zu können.

Wenn man mal guckt, wer da noch dazuzählt, da frag ich mich, ob das wirklich gerechtfertigt ist. Das muss ja nur jemand sein, der in der Nähe einer Autobahn oder alleine in einem Hochhaus wohnt. Wenn das alles die Aufgreifkriterien sind, dann ist das schon eine ganz gute Zumutung für das bisschen Erfolg, der dabei herauskommt. Das sind dann ja bestens Einzelerfolge.

Aber es sind ja nicht nur die einzelnen Sachen, es fallen ja noch mehr Kriterien da rein und dabei findet ja immer wieder ein Ausschluss statt und es bleiben nur wenige Leute über. Man fängt ja erst einmal an nach einem Kriterium zu suchen, wenn man das hat, hat man einen bestimmten Personenkreis. Da man aber mehrere Kriterien hat, fallen immer mehr Leute auch dadurch.

Aber es muss doch von jedem von uns eine große Anzahl von Daten vorliegen nur damit mal im Falle eines Falles auf einen Knopf drücken kann und damit das los geht. Das stört mich gewaltig an diesem Staatsdatentourismus. Aber, dass der Staat über alle so viel vorhalten muss, damit er im Zweifelsfall sagen kann, dass durch bestimmte Fragen oder Sortierfehler bestimmte Personen, die man haben möchte, herausfiltern kann.

Es stört ja erstmal keinen. Was mich an dem Datenmonster viel mehr stört ist, dass diese Daten für Dinge benutzt werden können, die nichts damit zu tun haben. Sind diese Daten, die da vorhanden sind nur für diese Zwecke da oder können sie auch anderweitig verwendet werden, also ein Missbrauch? Und überall, wo Personen sind oder wo sich einige Vorteile verschaffen können, muss man damit rechnen, dass sie dann dagegen verstoßen und dann einen Missbrauch stattfindet. Das beunruhigt mich mehr, als dass ich erst in ein Raster passe und nachher doch noch durchfalle.

Das ist doch einfach zu nett, dass die Daten gesammelt werden und man sie danach gebrauchen oder missbrauchen kann. Was erwarten Sie?

Erwarten tu ich es nicht.

Ich finde, dass die letzte terroristische Bedrohung München war. Wenn hier jemand vom Verfassungsschutz sitzen würde, dann könnte er Ihnen natürlich einiges dazu sagen, wahrscheinlich auch sehr aktuelle Dinge. Und es ist gut, dass sie nichts sagen dürfen, da das sonst verunsichern würde. Aber mit Sicherheit ist es nicht so lange her. Trotzdem bin ich der Meinung, dass die Privatsphäre ein enorm hohes Gut ist und dass dann auch eventuell die Sicherheit der Allgemeinheit darunter leiden muss. Alles, was erhoben werden kann, muss nicht erhoben werden. Und mein Vertrauen darin, dass wenn irgendwelche Daten erhoben

werden mit irgendwelchen Verfallsdaten, dass ich diejenigen die diese Daten verwalten dies auch tatsächlich tun, ist nahe zu null. Ich glaube auch nicht, dass Ihre Institution in der Lage ist, einen Bruchteil des Datenmissbrauches aufzudecken, was eigentlich Ihre Aufgabe ist. Ich glaube nicht, dass Sie erfolgreich sind. Ich bezweifle, dass Sie erfolgreich sind. Und Sie würden, wenn Sie mehr Personal hätten, deutlich mehr finden. Und deswegen bin ich extrem skeptisch. Ich meine nicht nur die Unternehmen, sondern auch Behörden, dass es da gesetzlich Grundlagen gibt. Da mag der eine oder andere darauf vertrauen, auch da bin ich skeptisch, dass die auch von solchen Stellen immer, bestimmt nicht beabsichtigt, aber so aus dem täglichen Leben beachtet werden und das geht unter.

Eine Frage noch. Findet denn bei diesen sicherheitskritischen Daten, um die es geht und die ja schon wie diese Terrordatei existieren, finden da überhaupt eine Kontrolle statt oder sammeln die einfach wild drauf los?

Noch eine Bemerkung zu dem Projekt. Es wurde eine Projektskizze verteilt oder uns zugeschickt. Und dann waren das 800.000 €, wenn ich das richtig gelesen habe. Und den Zuschlag haben die Österreicher bekommen. Es sind 6 Mitgliedsstaaten dabei. Ich persönlich habe die Befürchtung und hoffe, dass das nicht eintrifft, dass hier die EU ein Projekt vergeben hat, was in diesen 6 Staaten gemacht wird und alles ist auch eingehalten worden. Die Ergebnisse werden in allen Staaten mühevoll zusammenzufassen, das wird dann durchgelesen. Wir haben das, was wir auch vorher schon hatten und jetzt kann es durchgesetzt werden. Die Befürchtung habe ich.

Ich habe weitere Fragen. Sehen Sie positive Auswirkungen oder Einsatzmöglichkeiten von Sicherheitstechnologien? Fühlen Sie sich durch den Einsatz bestimmter Technologien besser oder sicherer?

Ich glaube, dass es in Notfallsituationen ganz gut sein kann. Dieses eCall, das würde sich lohnen, wenn man zum Beispiel irgendwo in einem Dorf liegt und mich niemand findet. Und sich dieses Ding dann einschaltet, fühle ich mich auch ein bisschen sicherer, aber man kann mich auch jederzeit orten.

Ich glaube, dass es denn wieder sehr konstruiert ist. Aber wenn du dein Handy bei dir hast, dann ist auch die Ortung sowieso möglich. Die Ortung ist ja auch personenbezogen und nicht auf das Auto. Also ich denke, dass man bei dem Handy viel größere Bedenken haben müsste.

Klar, das mit dem Handy ist auch noch so eine Sache.

Das sind theoretische Ortungsmöglichkeiten, die sehr strikten Vorgaben unterliegen, das heißt, dass die Polizei nicht einfach jedes Handy orten kann, sondern sie braucht einen richterliche Beschluss dafür.

Das Handy ist ja Schnee von gestern. Das mit dem eCall soll ja erst entwickelt werden. Und wenn ich der Besitzer eines kostbaren Wagens wäre, und es gestohlen werden würde, würde ich mich freuen, wenn ich es recht schnell wiederbekäme. In diesem Fall wäre es gut. Aber, wenn dann jede KFZ-Bewegung aufgezeichnet wird, dann ist mir der Preis zu hoch und ich nehme lieber den Verlust des Wagens in Kauf.

Können die Ortungsbehörden einen denn auch im Ausland orten, wenn man mit solch einem Wagen erst über die Grenzen von Deutschland hinaus ist? Da ist dann ja wahrscheinlich auch ein anderes Rechtssystem.

Auch der Falsche, der gerade ihr Auto sucht, findet Sie ganz schnell.

Der würde Sie dann auch schnell finden, weil er in dieses System eingedrungen ist.

Wenn auch eine Neuwagen das mal erhalten sollen, das sind dann ja einige Tausend und man wird ja nicht alle beobachten. Man wird ja einen Grund haben, ein Fahrzeug zu suchen und davon ist ja nicht jeder einzelne betroffen. Wenn da die Möglichkeit eingeschränkt wird, dass nur ein kleiner Personenkreis oder durch einen richterlichen Beschluss diese Möglichkeiten hat, dann hat es seinen Nutzen.

Nutzen hat es viel. Schon für die Versicherung, man findet den Wagen mit E-call wieder und die müssen nicht zahlen. Das würde mich nur wenig trösten. Wenn ich aber einen Container wiederfinden könnte, der mit definierten Umweltchemikalien relativ schnell wiedergefunden werden soll und auch eine öffentliche Bedrohung darstellt, dann würde ich es gar nicht schlecht finden, wenn man ihn schnell wiederfindet. Aber wenn da ein Container mit Computern ins Wasser fällt und das kommt ja schon häufiger mal vor, dann ist das der Preis für Datenschutz.

Wenn ich noch was dazu sagen darf. Sie sagen jetzt so blauäugig, dass man jetzt nicht alle Daten speichern kann und es ist ja auf einen bestimmten Personenkreis begrenzt. Also ich sag immer, die Technologie ist da und sie macht weiterhin Fortschritte und wir haben dieses System. Man hat es erst bei diesen Mautbrücken auf der Autobahn gesehen. Da hieß es erst, es werde nur LKWs überprüft und alles andere wird gelöscht. Und dann kommt der Innenminister und sagt die Daten existieren doch noch. Es wäre doch blöd die Daten wegzuworfen. Und ich denke, dass es dann auch so mit dem eCall sein wird. Gesetze sind sehr schnell aufgeweicht. Wenn die Bedrohung da ist, fallen alle Grenzen. Und die Technik ist so weit, dass man nachher alle Bewegungen der Autos aufzeichnen kann. Das Problem ist, wenn man erst mal diese Überwachungsmöglichkeiten hat, dann braucht man nur den Computer anschalten und dann hat man diese Daten.

Aber Sie brauchen ja in Ihrem ganzen Leben nie davon betroffen sein, sie können aber.

Irgendjemand wird immer betroffen sein.

Aber es werden doch nicht alle Besitzer gleichzeitig überwacht. Oder einige überhaupt nicht überwacht.

Ich finde es sollte auch noch immer die Möglichkeit vorhanden sein, sein Handy oder auch eCall auszuschalten.

Was heißt es, dieses eCall auszuschalten? Also, wenn ich es ausschalte, vergesse ich es sowieso wieder einzuschalten. Aber, wenn man jetzt diesen Sicherheitsaspekt bedenkt, hätte ich ein schlechtes Gewissen, wenn es aus ist. Was ist denn, wenn ich jetzt gegen einen Baum fahre? Das finde ich dann wieder schwierig.

Also, wenn ich dann durch die Stadt fahre, muss ich es ja nicht unbedingt an haben. Die Wahrscheinlichkeit, dass da jemand einen Notruf abgibt ist da höher als...

Das ist ja wie bei dem Airbag, den kann man auch ausschalten, damit man nicht rauskommt. Genauso kann man tagsüber mit Licht Auto fahren oder auch ohne, was noch die meisten in Deutschland machen. Es ist eben eine Grundeinstellung.

Und wenn man es auch abschalten kann, dann wird wahrscheinlich wenn ich jetzt an die Terrorbekämpfung denke, auch mit protokolliert, dass das Gerät abgeschaltet ist. Und dann ist es leicht in ein Raster zu passen. Entweder man gehört dann dazu oder man wird auffällig, weil das Gerät abgeschaltet war. Es sagt ja auch etwas aus, wenn man dieses Gerät abschaltet.

Ich hab mal irgendwie gehört, dass man beim Telefon, bei der Entwicklung dieser Mobilteile, die man zu Hause hat, dass es so einen DECT-Standard gibt und die ersten, die von der Industrie entwickelt worden sind, waren abhörsicher. Dann hat der Staat gesagt, dass die Technik es ein wenig übertrieben hätte und es doch nicht so sicher sein soll. Dann wurde eine Technik eingebaut, die dem Kunden sagte, dass der Nachbar das möglicherweise nicht abhören kann, aber möglicherweise einige Fachpersonen. Aber derjenige, der das kauft, liest abhörsicher. Für die Masse, für den Unkundigen abhörsicher.

Das haben sie auch bei W-LAN, das ist ja dasselbe Problem. Da kann man ja genauso rein.

Der Datenverkehr kann immer beim Kommunikationsanbieter oder dem Internetanbieter mitgeschnitten werden. Aber das Funktelefonieren, sozusagen, dass kann man absichern.

Aber nicht verbessern.

Bei diesem W-LAN da gehört ja immer noch eine lokale Nähe dazu. Beim Telefonanbieter spricht dann wieder nichts dagegen. Erstmal alles mitzuschneiden. Man müsste schon sehr verdächtig sein, wenn man sich mit einer Antenne vor das Haus setzt, um mal zu sehen, was funkt denn der so.

Aber da bin ich der Meinung, dass es da so viele Leute gibt, die andere beobachten. Warum sollte es nicht auch solche geben, die andere abhören. Auch bei den Einbrüchen werden die Leute vorher auch ganz genau beobachtet. Und dann wird irgendwann eingestiegen. Und das ist dann ja auch über Funkverbindungen möglich. Die Leute, die das wollen, haben auch die Technik dazu.

Wir haben auch noch die negativen Folgen und Auswirkungen, die Sie auch schon angesprochen haben. Wann ist der Einsatz dieser Technik nicht mehr akzeptabel? Haben sie eher sich oder auch das Gemeinwohl im Hinterkopf, wenn sie selbst betroffen sind? Hilft dann die Technologie weiter?

Die Terrorbekämpfung muss nicht unbedingt schon in der Umkleide anfangen. Beim Flughafen oder bei größeren Bahnhöfen muss man die Privatinteressen wahrscheinlich zurückstellen.

Oder auch der Weg, der von Gaarden über die Brücke führt, wo Leute überfallen wurden. Da muss ich eben damit rechnen, dass da mehr überwacht wird. Die Polizei überwacht die Gegend

auch nicht mehr und dann nehmen sich einige Leute immer mehr raus und dann kann es schon mal zu meiner Sicherheit sein.

Aber nicht automatisch jeder öffentliche Platz.

Nein, das muss es ja nicht sein. Gefährdete Bereiche.

Auch wenn da eine Kamera ist, heißt es ja nicht, dass dahinter eine Person sitzt und die ganze Zeit nur Verbrechen beobachtet. Bloß, weil die Kamera da steht, versucht man die Leute abzuschrecken. Das soll so ein bisschen Pseudosicherheit geben. Im Zweifelsfall passiert dann genauso wenig. Natürlich gibt es da Attrappen...

Das Problem ist ja auch, wenn man immer mehr Kameras anbringt, kann man gar nicht alle überblicken. Die Leute wissen das ja auch. Und je mehr Kameras vorhanden sind, desto geringer ist die Chance wirklich ein Verbrechen zu beobachten. Es wird für die Kameras nicht mehr Personal geben. Ich denke nicht, dass die Computer das erkennen können. Deswegen ist das auch trügerische Sicherheit.

Ja, aber es besteht auch die Möglichkeit, auch wenn man das Verbrechen nicht unbedingt verhindern kann, dass man im Nachhinein den Täter erfassen kann. Und das ist doch wichtig, diese Menschen von der Straße zu holen.

Und dann klebt einer die Linse der Kamera zu und dann ist es dunkel. Das ist doch nicht so, dass es eine gute Sicherheit ist. Derjenige, der da was vor hat, der weiß doch auch worauf er sich einlässt. Wenn die Kameras auf 3 Meter Höhe gesetzt werden dann kann man sie zwar nicht mehr zu kleben, aber es bringt auch nicht viel. Das ist doch nur ein andauerndes hinterherrennen der einzelnen Personen.

Das ist keine sofortige Sicherheit, sondern meiner Erachtung eine Erleichterung der späteren Strafverfolgung.

Aber die Frage ist ja auch, wen man da schnappt? Immer die Dummen und die die so ausgeheckt sind bleiben wieder unerkannt.

Aber es ist ja auch so, dass nachher dort, wo eben diese Kameras angebracht sind, dass gefilmt wird, und dann sieht man, dass da jemand mit einem Stock auf die Kamera schlägt. Und es wird dann eher sogar noch vor den Kameras etwas passieren, weil man dann ja Publikum hat.

Die Hemmschwelle, Straftaten vor Kameras zu begehen ist ja auch stark zurückgegangen.

Wenn man sich hier in Kiel die Autobahnauffahrten ansieht, sind überall Kameras. Diese sind ja eigentlich für die Ampelschaltung gedacht und es wird darauf geachtet, ob da irgendein Stau ist. Wenn man dieses nun mit dem neuen Kennzeichenerkennungsgerät, dann brauch ich gar nicht mehr eCall, dann kann ich das ja auch schon so sehen. Wer fährt gerade wo ist dann schon mal festgestellt und mit Hilfe eines schlaunen Programms, weiß ich dann genau, wo ich auf die Autobahn rauf und wo herunter gefahren bin. Wenn man jetzt noch die Mauttechnik und eCall zusammen vernetzt, dann fahren Sie keinen Meter mehr ohne, dass nicht festgestellt werden könnte, wie Sie gefahren sind.

Momentan kann man sowieso nicht sehen, nur beim Auswerten im Nachhinein.

Es ist ja auch so bei der Auswertung von solchen Massen an Daten, selbst, wenn man die Fehlerquote beachtet, wenn denn da einer falsch verdächtigt wird, ist bei dieser Menge schon viel.

Ich bin mal Opfer einer solchen Falscherkennung gewesen. Und habe dann auch gesagt, dass sie sich dann auch noch mal entschuldigen könnten, aber das taten sie nicht. Und wird dann die Akte verbrannt? Nein, die Akte ist abgeschlossen und wir haben uns geirrt. Und diese Akte existiert heute immer noch.

Ein ganz nettes Gedankenbeispiel ist da auch die Kinderpornografie. Wenn man da mal verdächtigt wird, selbst wenn man da frei gesprochen wird, muss man sich schon eine neue Nachbarschaft suchen. Am besten auch ein neues Bundesland. Und bei diesem Gedankenexperiment ist es so, dass man ja irgendwo auftaucht in Verbindung mit Kinderpornografie. Das wird irgendwo abgespeichert und bleibt auch dort. Wenn das gespeichert wird, kann ich mir vorstellen, dass man dann in eine Spirale gelangt, dass man dann wiedererkannt wird und man dann zweimal drinsteht und dann wird man immer wiedererkannt, wenn dann irgendwie unscharf gesucht wird.

Wollen wir doch erstmal sehen, wer besser passt, nehmen wir doch erstmal den.

Wenn ich jetzt an die Engländer denke in Portugal. Denen ist das momentan so was von egal, die wollen nur ihr Kind wieder haben. Wenn man eben selbst betroffen ist, gilt das alles nicht mehr. Da bin ich mir ziemlich sicher.

Ja, natürlich. Ich würde auch nicht anders reagieren.

Man sagt immer lieber nicht, aber wenn man dann betroffen ist, dann denkt man auch anders.

Es ist ja auch schwierig zu argumentieren. Dieses System, auch wenn es nur ein einziges Kind rettet, soll man denn sagen man darf es nicht einführen? Dann sagt man wirklich, was ist das bisschen Freiheit gegen das Leben dieses Kindes.

Wie werden in Deutschland eigentlich Datenschutzvergehen, auch kleinere, behandelt? Ist das schmerzhaft? Schreckt das ab?

Leider nicht.

Das war ja auch mein Punkt, als ich vorhin sagte der Schutz vor Missbrauch müsste verbessert werden. Aus meiner Sicht müsste es auch für solche Taten höhere Strafen geben. Die Anwälte sind da ja anderer Meinung.

Was die Unternehmen eher fürchten ist der Imageverlust.

Die Strafe muss ja nicht mal das Abschreckende sein, sondern eher das Urteil, das öffentlich verbreitet wird.

Wie oft habe ich da schon so eine Computerstimme am Telefon gehabt, die mir dann gratuliert hat, weil ich gewonnen habe. Aber auch bei solchen anrufen forscht man nicht genauer nach, was das denn war.

Noch eine Frage habe ich an Sie. Habe Sie eine Meinung dazu, wer daran beteiligt sein sollte, wenn Entscheidungen über den Einsatz von Sicherheitstechnologien getroffen werden?

Bei der Politik habe ich ja manchmal den Eindruck, dass sie versprechen, dass ihre Technologie bestimmte Sachen kann. Dann sagen die Politiker, dass sie das machen werden. Da würde ich mir wünschen, dass eher auf Sachverständige gehört wird und nicht nur Alternativen gesucht werden, sondern gewisse Projekte auch ganz gekippt werden.

Ich finde auch, dass es wichtig ist, dass da Experten dahinterstehen. Der Bürger kann ja nicht richtig mitverfolgen worum es da geht, wenn man nur irgendwelche Leute darüber reden und entscheiden lässt.

Ich sehe das so, dass der Politiker eigentlich nur Mittel zum Zweck bestimmter Interessensgruppen ist, weil er eben unkundig ist. Auch wenn er nach außen immer zeigt, dass er Sachverstand hätte. Aber wenn man das hinterleuchtet, sieht man, dass die Firmen oder Unternehmen dahinterstehen.

Er wird die Meinung des Volkes vertreten.

Aber das tut er ja nicht. Er vertritt die Interessen bestimmter Gruppen.

Er wird das vertreten, was eben am besten wirkt.

Vor allem muss auch der Sachverstand sehr stark berücksichtigt werden. Ich hatte letzten mit einer gesprochen, die sagte im Bundestag sei es so, dass sie viele Gutachten eingeholt hatten und auch vor den Abgeordneten lagen, aber niemand hat auch nur einen Blick daraufgeworfen. Dennoch haben alle mit abgestimmt. Ich denke, dass daran etwas geändert werden muss. Das die Experten gewisse Veto-Rechte haben.

Haben Sie Vorschläge zur Entwicklung und zum Einsatz von Sicherheitstechnologien? Was muss geändert werden? Was wäre noch denkbar, um Vorgaben zu machen?

Es wurde ja auch die Frage gestellt, ob diejenigen, die diese Technologie herstellen auch angehört werden sollen, weil die natürlich auch sagen können, welche Vor- und Nachteile so ein System hat, was sie gerade anbieten oder was generell technisch möglich ist und welche Gefahren dahinter stecken und wie ausbaufähig diese sind. Und das sollte man bevor man sich entscheidet, schon einmal gehört haben.

Hat sich in Ihrer Wahrnehmung zu diesem Thema durch diese Veranstaltung etwas geändert? Oder haben Sie sich damit schon länger befasst?

Ich habe bei der vorletzten Frage mit nein beantwortet. Es war gut, dass man das hier mal alles gebündelt bespricht, aber, dass sich meine Einstellung geändert hat, kann ich nicht sagen.

Ich bin relativ glücklich. Ich habe mich erst damit befasst, als ich auf die Uni ging und mich dann auch für Recht entschieden habe. Vorher habe ich immer gedacht, dass die Leute das schon machen und habe mich auch auf diese verlassen. In meinem Bekanntenkreis gibt es bestimmt immer noch solche, die das jetzt nicht so schlimm empfinden in solch einer Datenbank zu stehen. Das betrifft mich doch jetzt nicht.

Aber ich muss mich auch wundern, wie die auffallend ablehnende Haltung in dieser Gruppe aussieht. Ich dachte eigentlich, dass das weniger der Fall wäre. Ich bin einigermaßen vom Fach, ich bin Informatiker und habe mich entsprechend schon mal in das Thema eingelesen.

Wir haben 2000 Kieler Bürger angeschrieben, die ich zufällig aus dem Telefonbuch entnommen habe. Es haben sich die Personen gemeldet, die Interesse an diesem Thema haben.

Das was mich zuletzt beschäftigt hat zum Thema Datensammeln, war als meine Krankenkasse mich angerufen hat, um zu fragen in welchem Sportverein ich denn wäre. Und das ist ja freiwillige Datensammlung. Es wird ja auch an der Kasse gefragt, welche Postleitzahl man hat und das ist je alles, genauso wie eine Kundenkarte bei Karstadt zum Beispiel, freiwillige Datensammlung. Ob diese Daten wirklich von Nutzen sind, das bezweifle ich, aber bei einigen geht es dann schon an die Substanz.

Bei der Versicherung kann ich das Nachvollziehen. Das Rabattversprechen, was bei Kundenkarten dahintersteht, das ist der fühlbare Vorteil für Sie. Und es wird ein Kundenprofil erstellt, um Sie dann genauer mit Werbung ansprechen zu können.

Ja, einmal die Werbung, aber auch, um das Angebot besser abstimmen zu können. Und man sollte sich überlegen, ob man das preisgibt.

Ja, es werden ja so viele Daten misshandelt und verkauft...

Das finde ich schon bedenklich.

Und da besteht ja auch die Gefahr, dass sie versuchen werden an solche Datenbanken zu gelangen. Und dann wird es dem einen oder anderen Mitarbeiter nachher leicht gemacht, dagegen zu verstoßen.

In den USA gibt es eine Informationspflicht, das heißt, wenn in einem Unternehmen ein Datenmissbrauch stattgefunden hat, muss man die Öffentlichkeit benachrichtigen. Und jede Person, die betroffen sein könnte, anschreiben, um den Schaden zu begrenzen.

So ein Datensatz merkt ja nicht wirklich, wenn er kopiert wird.

Group 2

Ich frag einfach mal in die Runde. Was fällt Ihnen spontan zu den Begriffen Sicherheitstechnologie und Privatsphäre ein?

Was uns spontan einfällt?

Genau.

Außer dass ich jetzt viel darüber gelesen habe, geht es mir vor allem um diese Möglichkeiten, viele einzelne Daten zusammen zu sammeln und daraus denn die verschiedenen Charaktere bilden zu können. Das ist das, was mir am meisten im Gedächtnis geblieben ist und was ich dann als gespenstisch empfinde.

Also Profilbildung im weiteren Sinne.

Bei mir ist das so, dass man langsam Angst bekommt vor dem Ganzen. Vor allem, was da alles passiert. Ich kann mich zum Teil nicht wehren, weil das automatisch gemacht wird. Und privat möchte ich nicht, dass mir ja jemand ins Zimmer sieht oder meine Telefongespräche abhört. Ich finde, dass es auch ein bisschen zu weit geht, wenn man abspeichern könnte, wo man sich gerade aufhält. Wenn es gerichtlich beschlossen wäre, dann habe ich auch nichts dagegen. Bei Terroristen zum Beispiel, aber bei ganz privaten Bürgern geht das zu weit, aber das sind sie meisten auch. Ich weiß nicht, wo ich da eine Grenze ziehen soll. Wenn ich da eine Entscheidung treffen sollte, müsste ich passen.

Das ist genau das Spannungsfeld, um das es hier geht. Das ist genau diese Abwägung zwischen diesen beiden Gebieten.

Da möchte ich keine Entscheidung treffen.

Ich kann jetzt auch nur über die Grundeinstellung was entscheiden. Es liegt vielleicht aber auch daran, dass ich ein bisschen naiv oder staatsreu bin und immer eher denke, was der Sicherheit dient, ist auch in Ordnung. Von daher verstehe ich manche Diskussionen nicht, warum sich die Menschen darüber aufregen, wo ich meine, dass es größere Gefahren für den Menschen gibt, als jetzt ein paar Daten preiszugeben. Deshalb wunder ich mich manchmal, warum sich die Leute so aufregen.

Man kann heutzutage ja gar nicht verhindern, dass Daten über einen gespeichert werden. Also man kommt damit täglich in Berührung, außer, wenn man sich davor zurückzieht. Und was mir sehr wichtig wäre, ist, dass man ein Auge auf diesen Missbrauch solcher Daten hat, um eben dieses zu verhindern. Dass diese Verletzung des Datenschutzes eingebunden wird.

Ich lebe in einer Umwelt und diese Umwelt hat sich natürlich in den Jahren, in denen ich lebe extrem verändert. Und den Begriff Terrorismus kannte man früher ja noch nicht, jetzt kennt man ihn und mit diesem Begriff ist ja auch die Sicherheit verbunden, die jeder gerne haben möchte. Und deshalb bin ich der Meinung, dass alles was über ein Gericht läuft, ist für mich in Ordnung. Auch was gesagt wurde, was meine Privatsphäre betrifft, da bin ich nicht einverstanden. Da bin ich sogar extrem dagegen, dass da Daten benutzt werden, die aber dem Staat zur Verfügung stehen sollen.

Das ist schon mal ein wichtiger Punkt zwischen Staat und Wirtschaft zu unterscheiden. Sie haben ja im Vorfeld der Befragung alle diese Szenarien bekommen, in dem die beiden Herrschaften zum Flughafen oder auch Bahnhof fahren, um jemanden zu besuchen. Haben Sie etwas zu diesen Szenarien zu sagen? Ist Ihnen etwas aufgefallen? Wie fanden Sie diese Szenarien?

Teilweise schon ein bisschen übertrieben. So empfinde ich das auf jeden Fall.

Können Sie das ein wenig spezifizieren?

Ja, das kann ich nicht sagen. Da sind so viele Sachen drinnen gewesen, die man einfach schluckte und so akzeptierte. Was mir dabei auffiel, war das mit dem Auto, dass man das überwachen kann, dass ich denn mal zu schnell fahre, dass das dann immer gleich vom Konto abgebucht werden kann. Das finde ich schon ein bisschen hart. Das war für mich ein Punkt, bei dem ich dachte, dass ist dann doch ein bisschen viel. Irgendwo muss ja eine Grenze sein.

Das ist ja ein zukünftiges Szenario. Diese Technik wird jetzt langsam eingeführt. Die Möglichkeit, es für Temposünder zu verwenden ist erstmal nur potentiell möglich, was aber erstmal nicht geplant ist.

Aber wenn man so was schon mal in Angriff genommen hat, dann dauert es meistens auch nicht lange. Bei mir war es so, dass ich vorher erstmal gelacht habe, weil ich es als unmöglich empfand, dass der Staat so was zulässt. Aber ich habe einen Unfall gesehen, wo ein Raser einen völlig Unbeteiligten dann umgerast hat. Und seitdem habe ich meine Meinung verändert und bin in dieser Richtung sehr viel konservativer geworden. Früher bekam ich einen Adrenalinstoß, wenn mich jemand überholte und meinte ich müsste auch hinterher, aber die Zeiten sind vorbei. Aber wenn einer in einer 60-Kilometerzone mit 100 durchrast, dann sollte man den ruhig anhalten können.

Ja, anhalten schon. Aber wenn das System gleich sagt, dass du zu schnell gefahren bist und du dann gleich drei Punkte in Flensburg bekommst und von deinem Konto 100 Euro abgebogen werden. Da habe ich was gegen. Aber wenn die Polizei da mit einem Wagen steht und die Technik hat, so etwas jetzt ein wenig leichter zu messen, dann habe ich nichts dagegen.

Hätten Sie was dagegen, wenn jetzt zum Beispiel eine Warnlampe angeht, sobald jemand das Tempolimit um eine gewisse Höhe überschreitet?

So dass ich das bei meinem Auto merke?

Nein, generell. Das klang gerade so, dass Sie dafür wäre, wenn jemand deutlich zu schnell fährt, sind Sie dann der Meinung, dass so ein System das automatisch melden sollte und den Wagen dann irgendwie anhält oder runterbremst?

Ja, das war ja früher so bei den LKW. Früher bin ich LKW gefahren und da war es wirklich so, dass es eine Motorbremse gab und man nicht schneller fahren konnte. Es ging eben nicht schneller.

Also ich möchte noch mal auf die Szenarien zurückkommen. Was mir dabei im Gedächtnis geblieben ist, das sind diese vielen Gedanken, die sich diese beiden Menschen auf dem Weg dahin machen. Ich habe mir auch viel unterstrichen. Dass es halt diese vielen verschiedenen Dinge gibt und dass sie im Wesentlichen für unsere Sicherheit da sind und um sie zu verbessern. Da habe ich auch noch das Problem dabei, dass ich dem Staat nicht so blind vertraue, dass diese Dinge wirklich gut sind, weil ich da schon viele Dinge gehört habe, dass das teilweise gar nicht so ist. Was diese biometrischen Pässe angeht, da habe ich viele verschiedene Dinge gehört, dass das nicht unbedingt dazu dient unser Leben sicherer zu machen.

Sie haben also an der Sinnhaftigkeit der Technik Zweifel?

Ich habe Zweifel daran, dass es dazu da ist unser Leben sicherer zu machen, indem wir mehr überwacht werden. Das kann ich mir nicht vorstellen.

Wozu vermuten Sie wird die Technik denn dann eingesetzt, wenn nicht zur Terrorbekämpfung dient?

Weil es sie gibt und weil auch viele Firmen gut daran verdienen, wenn überall eingebaut wird. So soll zum Beispiel Siemens diese Biometrischen Pässe entwickeln und auch marktfähig machen. Und die freuen sich natürlich darüber, dass sie das dürfen.

Was mir allerdings aufgefallen ist, dass es irgendwie alles wie Science-Fiction wirkt, weil da auf einmal ganz viele Sachen kommen, die einem neu und unbekannt sind. Ich glaube, dass man ganz anders darüber denken würde, wenn man in dieser Zeit leben würde, in der die Sachen immer nur peu à peu dazukommen würden und man das nicht wahrnehmen würde, die dann einfach dazugehören. Es ist dann einfach eine Entwicklung in meinem Leben, die in der Vergangenheit auch schon stattgefunden hat. Wir leben jetzt auch in einer Zeit, wo viele Dinge mit Kamera überwacht werden und welche Frage ich mir gestellt habe, ist, wo das alles einmal enden wird. Irgendwann könnte es ja rein technologisch möglich sein, dass man in die Gedanken eine Menschen hineinsehen kann und dann auch in den Gedanken überwacht werden kann. Das ist eben ein Punkt, an dem man abwägen muss, was wirklich sinnvoll ist und was nicht eben blind durchgesetzt wird, nur weil man die Technologie hat. Man will zwar keine Rückschritte, aber irgendwie wollen die Firmen, die diese Technik entwickeln auch anwenden.

Ich muss auch daran denken, dass diese Pässe überhaupt nichts bringen würden bei Schläfern, die ihr Leben lang ruhig irgendwo sitzen und sich als Studenten ausgeben und dann mit einem völlig legalen Pass dadurch kommen. Und dann trotzdem ihren Auftrag erfüllen können. Da bin ich der Meinung, dass das überhaupt gar nichts bringt.

Aber in dem Moment wo man überwacht, dass das dann eine Firma übernimmt diese Technologie dann auszubauen und dem Staat zu übergeben, das ist ein normaler Zug. Als ich Kind war hat man sich geprügelt, bis einer auf dem Boden lag, dann hörte man auf. Aber es hat sich ja die Hemmschwelle beim Menschen stark verändert. Ich fühle mich nicht überwacht, wenn eine Kamera auf mich zeigt. Heute haben wir ja von dem Prozess in Potsdam mit dem Äthiopier gehört, dass die Angeklagten freigesprochen wurden, weil sie sich nicht sicher waren, wer es war. Wenn die es wirklich gewesen sind, dann waren sie eben gut. Die haben bis zum gezeugnet und niemandem etwas erzählt. Ich meine, dass sich durch diese Globalisierung und das Verändern der Lebensweise auch meine Umwelt verändert hat. Ich erwarte vom Staat, dass er mich schützt und dass ich auch für diesen etwas abgeben muss, aber keine kommerziellen Mittel. Eigentlich da, worum es darum geht Geschwindigkeiten zu überschreiten, da darf der Staat nicht eingreifen, aber letzten Endes werden dadurch auch andere gefährdet. Und seitdem habe ich auch meine Meinung geändert. Aber wenn man einmal gesehen hat, dass eine unbeteiligte Person in einen Unfall verwickelt ist, dann kann der Staat nach meiner Meinung ruhig was tun.

Also wäre es für Sie ein positiver Aspekt von Sicherheitstechnologien das Leben anderer zu beschützen?

Vielleicht hängt das auch mit dem Alter zusammen. Vor einem Jahr hätte ich es mir noch gar nicht vorstellen können, dass ich diese Denkweise entwickeln werde. Aber dadurch, dass ich

viel im Ausland gewesen bin, weiß ich auch wie gut wir es hier haben. Fahren Sie mal woanders hin.

Im Bezug auf was?

Sicherheit. Wenn Sie aus dem Hotel herausgehen, dass dann der Portier fragt, wo Sie hin wollen. Oder er Ihnen einfach die nächste Kneipe nennt und Ihnen dann noch den Pagen als Begleitung anbietet. Sie sollen dann anrufen, wenn sie wieder zurück kommen wollen. Sowas haben wir in Deutschland nicht.

Ja, aber wo ist da eine Grenze?

Ja, das ist das Schwierige.

Auch wenn die Daten irgendwo gesichert werden, irgendwo müssen die Daten ja sein. Und dann kommt der Missbrauch dazu. Und es stand auch irgendwo drinnen, dass die Daten geklaut werden und dann für touristische Aktivitäten genutzt werden.

Und das gilt vor allem für biometrische Daten?

Ja, und wer passt da auf? Da müssen ja vier oder fünf Leute sein, die gleichzeitig zu dem Punkt Zugriff haben.

Wie würde das aussehen?

Es ist eigentlich relativ einfach. Wenn Sie ein biometrisches System haben, haben sie Ihren Daumen und das System kennt das Daumenmuster. Es hat im Idealfall kein Abbild Ihres Daumens, sondern kennt nur spezifische Punkte. Dann legen Sie Ihren Daumen drauf und das System macht ein Foto, macht aus dem Foto dann wieder ein paar Punkte und vergleicht dann diese Punkte miteinander. Wenn die Punkte stimmen, gibt es im System ein ok. Wenn es jemanden gelingt an das Punktemuster zu gelangen und es ihm gelingt, dem System einfach das Punktemuster einzuschleusen, also per Datenleitung einspielen, dann glaubt das System auch, dass das Punktmuster übereinstimmt und lässt denjenigen durch. Die andere Variante ist, dass jemand die Fläche, die sie gerade angefasst haben, nimmt und dann mit einfachen Haushaltsmitteln, wie Sekundenkleber, Leim und einem handelsüblichen Laserdrucker sich eine Fingerabdruckkopie an. Man kann auch mit dieser Kopie viele Lesegeräte überlisten. Das wäre dann der Missbrauch, der möglich wäre. Bei Fingerabdrücken ist es auch noch besonders leicht, weil wir überall unsere Fingerabdrücke hinterlassen.

Es kann auch umgedreht sein, dass ein Terrorist Ihren Daumenabdruck hat.

Und das Problem ist eben, dass sobald bei biometrischen Systemen die Template-Daten abhanden kommen, dann ist es jemandem zumindest theoretisch möglich diese Daten in ein anderes System einzuspeisen und diesem System vorzugaukeln, dass die Daten übereinstimmen. Da sie aber nur einen einzigen Daumen haben, ist der sozusagen verbrannt, sobald die Daten einmal weg sind. Das ist sozusagen das Missbrauchspotenzial des Systems.

Aber ich denke, wo diese Biometrie eingeführt wird, muss der Staat dafür sorgen, dass so was eben nicht geht. Und letzten Endes muss er bestimmte Forschungsaufträge an die Firmen geben und fragen, wie man das vermeiden kann. Das erwarte ich eigentlich auch vom Staat, dass

dafür Gelder zur Verfügung gestellt werden, um diesen Missbrauch von vorn herein auszuschließen. Davon gehe ich eigentlich aus.

Sie erwarten also eine neue Einführung von neuen Sicherheitstechnologien, die aber dann sehr sicher sein müssen?

So ist das.

Bisher ist ja immer jemand in die Datenbank eingedrungen.

So sehe ich das auch.

Das hat man ja mit den Hackern gesehen. Die besten Leute hätte man kaufen sollen, denn die kennen das System ja. Du bekommst von mir 500.00 Euro, jetzt pass mal auf. Da ist es ja genauso.

Das ist richtig. Aber der Staat zieht ja immer nach, weil man von vornherein ja noch nicht so genau weiß, was man fälschen kann. Erst wenn gefälscht wurde, sagt der Staat, dass man das ausschließen muss. Hier darf es nicht sein, hier darf der Staat nicht das Internet benutzt werden, wenn er Daten überträgt. Das muss ein völlig getrenntes Netz sein. Ob das alles möglich ist, das ist die Frage, aber das muss gemacht werden.

Sobald Menschen dabei sind, bin ich der Meinung, dass es passieren kann.

Ich würde vor allem nicht nur Fragen, ob es möglich ist, sondern ich würde gerne wissen, ob man das überhaupt braucht, ob man diese Daten braucht, ob man diese Muster braucht, wenn man Fingerabdrücke speichert, um dann noch mehr Geld auszugeben, dass dann an diese Technik niemand herankommt. Da finde ich, dass man da vorher einen Grund haben sollte, warum wir diese Daten abgeben sollen. Da könnte man das Geld, was sonst dafür ausgegeben wird eben für diese Sicherung besser verwenden.

Das klingt ja alles gut. Vor vierzig Jahren hätte ich genauso gedacht wie Sie. Ich habe aber schon eingesehen, dass sich in der Zwischenzeit das Leben für uns verändert hat. Und wenn der Staat den Auftrag von seiner Bevölkerung erhält einem Sicherheit zu geben, dann erwarte ich, dass er diese ganzen Technologien, die jetzt möglich sind uns zu schützen, davon geht man ja aus, auch ausnutzt. Das denn da die anderen Konsequenzen mit drinnen sind, wie Sie gesagt haben, ist leider so.

Ich fände es problematisch, wenn diese Technologien eingesetzt werden ohne, dass man auch mal guckt, ob das denn überhaupt Sinn macht. Ich habe so den Eindruck, dass mit diesen Daten ein neuer Super-PC eingeführt wird, den Siemens irgendwann mal herausbringen wird. Und sagt, wir haben das Neueste vom Neuesten und wollen das vielleicht auch ein bisschen antreiben, damit sie dann irgendwie schneller sind als irgendjemand anders, der das auch bauen möchte und vergessen dabei, dass da irgendwelche Fehler sind.

Sie meinen, dass dann Viren eingeschleust werden.

Da meine ich, dass man da nicht so darauf achten sollte, dass das jetzt so toll und neu ist, sondern, ob wir es wirklich brauchen. Da bin ich zumindest der Meinung, dass das fraglich ist.

Die biometrischen Daten in Reisepässen wurden doch hauptsächlich eingeführt, weil die Amerikaner wollten, dass man nur noch einreisen darf, wenn man solch einen Pass mit biometrischen Daten hat.

Ja, das war die Haupttriebfeder.

Und da ist ja sowieso die Frage, ob es Sinn macht. Gut, die Leute, die dahin wollen, die haben keine andere Möglichkeit. Da kann man ja selbst die Entscheidung treffen, ob es einem das wert ist, oder nicht. Aber man sollte sehr genau überlegen, ob es denn Sinn macht, das auf alle auszuweiten.

Ja gut, von Amerika haben wir nach dem Krieg den Kaugummi bekommen, dann die Blue Jeans, dann die Kriminalitätsraten und jetzt bekommen wir eben das, aber das ist eben der Lauf der Welt, glaube ich. Es hat sich eben alles so verändert und man kann nicht sagen, dass wir wieder so wie vor 40 Jahren leben wollen. Da würde ich auch sofort ja sagen. Aber wie viele Menschen flohen vor 40 Jahren nach Amerika? Wie viele Flugzeuge fliegen heute in die vereinigten Staaten?

Es muss bloß alles sicher werden, das ist das Problem.

Und wir brauchen natürlich nicht alles den Amerikanern nachzumachen. Man muss zwischen den Denkweisen der Amerikaner unterscheiden. Man hat die Regierung, die jetzt da ist und man hat die Bevölkerung. Und diese beiden Denkweisen sind völlig unterschiedlich. Aber die Amerikaner sind mit dem, was so gemacht wird in Bezug auf die Sicherheit auch mit einverstanden. Das können wir uns ja gar nicht vorstellen, für die ist der 11. September ein Trauma.

Was sind für Sie die negativen Aspekte von Sicherheitstechnologien?

Negative Aspekte...ich würde mich diesem Argument mit dem Sinn, da könnte ich mich der kritischen Haltung anschließen. Wenn es natürlich nur Geldverschwendung ist, wenn man den gleichen Finanzaufwand auf andere konventionellere Art und Weise Sicherheit schaffen kann, durch mehr Polizeipräsenz, dann würde ich auch eher dorthin tendieren.

Es überwiegen also die positiven Aspekte für Sie?

Ansonsten würde ich es auch so sehen, dass das, was technisch möglich ist und in irgendeiner Form hilft in Ordnung ist. Und dann auch gemacht werden sollte.

Sie stellen hauptsächlich die Sinnfrage voran. Und wenn die Sinnhaftigkeit bewiesen ist, dann...

Ja, also ich habe jetzt keine großen moralischen Bedenken, dass ich jetzt meine, dass mein Land untergeht oder dass sich die Gesellschaft zu sehr wandelt oder dass die Freiheit eingeschränkt ist. Das kann ich nicht immer ganz verstehen. Auch diese Überwachungssachen, die Polizei hat auch Waffen, die auch in die falschen Hände kommen können und dann passieren auch schlimme Dinge, aber das ist letztlich was viel Schlimmeres als wenn jetzt jemand weiß, wann ich wo war. Damit könnte man ja noch leben.

Das hat meine Frau auch gesagt. Die hat das besser als ich durchgelesen. Und die sagte, dass ich sagen solle, dass mehr Polizisten nachts durch die Straßen geschickt werden sollen. Da hat man eine bessere Sicherheit. Das stimmt natürlich nicht, aber ich glaube, dass das ein psychologischer Aspekt ist. Die Polizei hat heutzutage auf der Straße nicht mehr die Möglichkeiten wie früher. Das hat sich auch verändert.

Eine Videokamera hat aber auch nicht die Möglichkeit einen Verbrecher anzuspringen oder ich aufzuhalten.

Das nicht, aber irgendwo geht eine rote Lampe an.

Wir hatten schon herausgearbeitet, dass es ein Spannungsfeld zwischen Sicherheit und Privatsphäre gibt und dass man keine klare Grenze setzen kann. Unter welchen Bedingungen finden Sie Sicherheit wichtiger als Privatsphäre? Und unter welchen Bedingungen finden Sie Privatsphäre wichtiger als Sicherheit?

Wenn man selbst von irgendwelchen Leuten angegriffen wird, dann denkt man wahrscheinlich anders darüber. Ich weiß es nicht.

Pauschal würde ich auch sagen, dass mir, wenn ich alleine bin meine Privatsphäre wichtiger ist als meine Sicherheit, weil ich dafür dann selber verantwortlich sein kann. Sobald ich unter andere Menschen gehe, kann ich für meine Sicherheit nicht mehr verantwortlich sein. Und da würde ich tendenziell sagen, dass meine Sicherheit dann wichtiger ist. Ich habe zwar noch keine eigene Familie, aber das soll sich bald ändern. Da würde ich natürlich auch sagen, dass mir das wichtiger ist und dann würde ich auch Einschränkungen meiner Privatsphäre eher einsehen und damit leben können als jetzt. Ich denke, dass kommt auch immer ein bisschen auf die Situation an, in der man sich gerade befindet. Wenn ich für mich selbst sprechen kann, ist mir meine Privatsphäre eigentlich heilig. Da würde ich mich dagegen sträuben, dass da irgendwelche Sachen über mich gesammelt werden.

Aber was ist jetzt anders, wenn man Familie hat? Wo ist da jetzt der Sprung?

Na, ich glaube, dass man dann nicht mehr komplett alleine ist oder sein kann. Man hat sowieso Leute um sich herum, die wissen, was los ist, oder?

Ne, das sind einfach Leute, die mir wichtiger sind als ich selbst. Oder mindestens eben so wichtig.

Aber das kann man als Single doch auch. Ich meine, dass ich doch trotzdem an der Umwelt interessiert bin. Ob ich jetzt alleine bin oder nicht, da verstehe ich jetzt nicht den Unterschied.

Wenn ich jetzt zum Beispiel mit dem Zug fahren will, kann es ja immer sein, dass da jemand drinnen sitzt, der ein Zeichen setzen will und in seinem Koffer eine Bombe hat. Da würde ich mich natürlich besser fühlen, wenn da vorher schon ein bisschen geguckt werden würde. Allerdings würde ich dann auch genau wissen wollen, wonach geguckt wird. Da kommt dann auch wieder die Frage, ab wo man sagen kann, dass das zu viel ist. Ich würde sagen, dass mir nur dann die Privatsphäre komplett wichtiger als die Sicherheit ist, wenn ich komplett für mich alleine bin.

Also schätzen Sie in den eigenen vier Wänden die Privatsphäre mehr als außerhalb und in der Interaktion mit Menschen die Sicherheit.

Aber wie schützen Sie sich denn in Ihrer Privatsphäre? Wir haben Jalousien überall. Und die sind sehr schwierig aufzumachen, weil die aluminiumgesichert sind. Ich finde, dass Sicherheit, Privatsphäre und Überwachung drei Begriffe sind, die ganz schwer zusammenzubringen sind. Ich bin der Meinung, dass meine Privatsphäre nicht gestört wird, wenn ich überwacht werde. Natürlich nicht zu Hause, aber muss die Möglichkeit zu Hause haben mich blitzschnell überwachen zu lassen, wenn zum Beispiel eingebrochen wird, dass ich dann einen Knopf zum Drücken habe und dass dann jemand kommt. Mir ist aber auch schon passiert, dass die Polizei und vom Terminal jagte. Und eine Stunde später gab es dann einen großen Krach. Da hatten sie eine Kofferbombe gefunden, die sie dann zur Explosion gebracht hatten. Nachher ging man an dem Loch vorbei, weil man ja in das Flugzeug wollte. Wenn man so was überlebt, dann sagt man sich hinterher, dass einem die Sicherheit doch ein wenig wichtiger als die eigene Privatsphäre ist.

Das gilt aber grundsätzlich. Es gibt wenige Situationen, in denen Sie sagen würden, dass Ihnen da die Privatsphäre wichtiger als die Sicherheit ist.

Ich kann im Moment keine Grenzen zeichnen. Das weiß ich nicht. Keine Ahnung. Wenn ich zu Hause bin, möchte ich meine Privatsphäre haben, wenn ich draußen bin, habe ich die Umwelt um mich herum. Aber wo die Grenze ist, weiß ich nicht.

Möchten Sie noch Grenzen ziehen?

Ich würde auch so sagen, dass es in den eigenen vier Wänden wichtig ist unantastbar zu bleiben und an öffentlichen Plätzen finde ich es wichtig, dass, wenn dort überwacht wird, man darauf hingewiesen wird. Also, dass sich jeder bewusst wird, dass er überwacht wird, auch wenn man sich dadurch vielleicht auch ein wenig anders verhält. Und man weiß, dass es nicht nur irgendwelche Videokameras sind, sondern dass da irgendwelche Gesichtserkennungsprogramme eingebaut sind, die dann auch verhaltensauffällige Personen herausgreifen. Das geht schon wieder zu weit, wenn man das Gefühl hat, dass man sich draußen nicht mehr unbeschwert bewegen kann. Wir leben ja doch noch in einem Land, in dem wir relativ wenig Probleme mit Terrorismus haben. Ich finde, dass man das jetzt noch nicht übertreiben sollte. Wenn sich der Terrorismus jetzt häufen würde, dann müsste man sich natürlich auch überlegen, ob man da dann stärkere Sicherheitsmaßnahmen trifft. Aber ich sehe noch nicht den Handlungsbedarf, um jetzt extreme Sicherheitsvorkehrungen zu treffen.

Aber dann kann es irgendwann mal sein, dass es zu spät ist.

Na ja, gut, aber das Risiko muss man immer eingehen. Dann lieber ein blaues Auge kassieren als...Sonst kann man sich natürlich von vorn herein in eine grüne Gummizelle einpacken...Auch wenn man zu vorsichtig ist, kann man das Leben nicht mehr genießen. Das ist eben die Sache, dass man sich zu sehr einschränkt und sich zu sehr in diese Angstsituation lässt. Mir ist es auch schon mal passiert, dass ich in Berlin, wo man von vorn herein, wenn man in eine jüdische Einrichtung will, erst einmal gefilzt und durchleuchtet wird und das fand ich eben komisch, weil man immer den Gedanken hatte, dass man an einem Ort ist, der anscheinend so wichtig ist, dass diese Sicherheitsmaßnahmen notwendig sind.

Aber ist es nicht teilweise so, dass man gar nicht darüber nachdenkt. Wenn Sie durch die Mönckebergstraße gehen oder auch in Kiel sind Kameras angebracht, genauso wie im Parkhaus. Überall dort werden Sie gefilmt und das nehmen wir einfach so hin. Da denken wir schon gar nicht mehr drüber nach.

Die Tankstelle hat auch jedes Auto aufgenommen.

Irgendwann wird es auch so sein, dass man irgendwohin geht und sagt in Ordnung. Das ist so und man geht durch.

Der Aspekt, der gerade angesprochen wurde, war ja auch im Szenario beschrieben, dass Kamerasysteme mit einem Erkennungssystem gekoppelt werden, um auf diese Art und Weise Anomalien herauszufinden. Verändert sich das Verhalten von Menschen, wenn sie wissen, dass Anomalien automatisch in irgendwelche Raster fallen, wenn ich mich zum Beispiel hektisch bewege? Dann werde ich als Gefahrenobjekt klassifiziert, das heißt, dass ich mich nicht mehr hektisch bewegen werde. Ich gehe dann morgens früher aus dem Haus, damit ich nicht zum Bus laufen muss, nur damit die Kamera nicht denkt, dass ich etwas auf dem Kerbholz hätte. Das ist also die Fiktion dahinter.

Also, wenn ich ein Terrorist bin, dann weiß ich das. Dann geh ich also langsam. Und die Leute, die dann hinter einem Bus herlaufen, die machen sich keine Gedanken darüber. Aber die Terroristen, die wissen es ja. Die verhalten sich ganz normal. Das ist vielleicht eine Anomalie. Oder ich kann den Bus auch fahren lassen, wo jeder sagen würde, dass er hinterherlaufen würde. Durch ihre Frage bin ich das erste Mal auf so was gestoßen worden, dass man in diese Richtung denken könnte, ob die Kamera einen aufnimmt, oder nicht.

Ich wollte nur illustrieren, welche Möglichkeiten dahinterstehen. Das eine Kamera einen Menschen aufnimmt, ist die eine Sache, das landet dann auf irgendwelchen Bändern, die dann nach einer gewissen Zeit gelöscht und dann wieder neu beschrieben werden. Das stört viele nicht. Aber wie gesagt, der nächste Schritt wird diese Gesichtserkennung sein. Für Flughäfen und Fußballstadien arbeitet man schon an einer Bewegungserkennung. Das ist dann schon die nächste Stufe der ganzen Geschichte.

Mich würde es nicht stören. Ich habe da aber auch noch nie drüber nachgedacht. Aber alles, worüber man nicht nachdenken kann, geht nur in einem demokratischen Staat. Das könnte sich bei uns ja auch noch mal ändern, dann würde ich hier natürlich völlig anders diskutieren. Da können wir ja gar nicht diskutieren.

Da sind wir dann schon bei der nächsten Frage, die das Staatssystem betrifft. Wer sollte denn Ihrer Meinung nach mit einbezogen sein, wenn von staatlicher Seite Sicherheitstechnologien eingeführt werde? Wer sollte gehört werden? Wer sollte daran Mitspracherecht haben? Also zum Beispiel, welche Interessensgruppen? Bürgerrechtler? Welche politischen Verbände?

Keine.

Doch auf jeden Fall Bürgerrechtsgruppen. Die haben ja noch den Vorteil gegenüber der allgemeinen Bevölkerung, dass sie besser informiert sind und auch besser in dem Thema stecken und von daher auch eine fundiertere Meinung dazu haben und vielleicht sogar eine Contraposition zu dem Thema einnehmen können, um diesen goldenen Mittelweg zu finden.

Grundsätzlich würde ich jetzt mal unterstellen, dass der Staat dazu neigt zu hohe Sicherheitsstandards oder Zukunftstechnologien aufzubauen und dann irgendwo noch einen Pol ist, der das ganze ein bisschen kontrolliert und kritisch durchleuchtet und dann eventuell auch an die Öffentlichkeit geht. Wenn der Punkt kommen sollte, dass keiner das überwacht, sehe ich die Gefahr, dass sich das irgendwo verselbstständigt und letztendlich dann doch mehr Daten von uns aufgenommen werden oder gesammelt werden als uns lieb ist und dann jeder erstmal grundsätzlich verdächtigt wird. Und das finde ich, ist eben dieser Punkt, wo man halt nicht hinkommen darf, dass jeder Bürger erst mal grundsätzlich als Feind eingestuft wird.

Wissen Sie das, ob das jetzt schon gemacht wird?

Ich weiß nicht.

Wir sind ja ein demokratischer Staat und da sind bestimmte Rahmenbedingungen und so hoffe ich, dass die dann eingehalten werden.

Das hoffe ich auch.

Wir hätten dann auch die Presse, die dann auch dementsprechend Alarm schlagen würde.

Aber das dumme ist mit diesen ganzen Bürgerbewegungen, dass man das Gefühl hat, dass es so eine Selbstverwirklichung bei einigen Personen ist. Wenn man sich jetzt mal ins Gedächtnis ruft, was bei dem G8-Gipfel alles passiert ist. Ich möchte heute kein Polizist sein, sonst würde ich da auch zuschlagen. Aber was ich da im Fernsehen gesehen habe, wie die da mit Steinen beworfen wurden, dass nur deswegen die ganzen Kamerateams dort aufgetaucht sind. Das ist unmöglich. Ich hoffe eigentlich, dass unser Grundgesetz so ist, dass man den Politikern die Entscheidung, wie was läuft, dass man das denen anvertrauen kann.

Ich wollte auch gerade den G8-Gipfel als Beispiel nehmen. Allerdings dafür, wie man eine Diskussion führen kann ohne alle Betreffenden an den Tisch zu holen. Ich glaube, dass es eigentlich nur so laufen kann, dass man möglichst viele Leute mit einbezieht. Das man auch versucht zu gucken, ob das überhaupt für und alle schön ist, wenn wir alle immer mehr mit solchen Kameras überwacht werden.

Ja, das stimmt natürlich.

Das ist das eine. Das andere ist ja, dass das institutionalisiert ist. Das die verschiedenen Organisationen da mitreden müssen, würde ich jetzt auch nicht für notwendig erachten. Dass natürlich bevor so was eingeführt wird, die Regierung selbst prüft, was das für Aspekte sind, empfinde ich für selbstverständlich.

Es müssen eben alle auf einen Nenner kommen.

Wie ist es mit Sicherheitsfirmen? Sagen wir die Wirtschaft genauer gesagt.

Meinen Sie, dass denn da so ein Sicherheitsmann vor einem Juwelierladen steht?

Sollten Sicherheitsfirmen oder Sicherheitskonzerne bei der Einführung von Sicherheitstechnologien noch mit einbezogen werden?

Keine Kommerziellen, die dafür Geld verdienen. Nein, das muss der Staat machen.

Die entwickeln das doch im Schlaf.

Das dachte ich auch.

Sie können dann später eben auch den Auftrag vom Staat bekommen etwas zu entwickeln.

Ich glaube, dass zu solch einer Diskussion eigentlich jeder was beizutragen hätte. Selbst diese Firmen, die sagen könnten das und das können wir, das und das geht gar nicht.

Ach so. Ich dachte jetzt die die Sicherheitsüberwachung übernehmen, dass da die Leute...

Nein, bei der Einführung von Sicherheitstechnologien.

Wo wollen sie es denn sonst machen als zum Beispiel irgendwelche Unternehmen, wie Siemens, Universitäten oder Fachhochschulen. Da muss der Staat die Hardware für das Gerät haben. Also, ich kann mir das nicht vorstellen und ich habe auch angst davor, wenn private Unternehmen da mit drin stecken, da werden die Firmen gleich wieder verkauft. Und irgendein Fond in Großbritannien überwacht uns denn hier.

Sollte es generell irgendwelche Regulierungen geben? Nach welchen Regeln sollte das ganze ablaufen? Sollte es Beschränkungen in der Entwicklung geben? Sollte die Regierung grundsätzlich jede Sicherheitstechnologie, die es gibt einführen? Beschränkungen ist das Stichwort. Wenn ja, wo sollten Beschränkungen existieren.

Ich glaube, dass man das erst sagen kann, wenn man weiß, was für Sicherheitssysteme kommen sollen. Die vierte Macht sind ja die Medien und die erfahren ja eine ganze Menge früher solche Dinge und soll die Bürger einfach informieren. Und da muss der Staat irgendwie reagieren.

Es gibt aber auch einige Dinge, bei denen Die Medien ein Berichtverbot erhalten. Zum Beispiel die Kopierschutzsysteme. Es gibt eine Richtlinie nach der die Presse keine Berichte über Software veröffentlichen darf, die das Knacken von Kopierschutzsystemen ermöglichen. An der Stelle, wird, so sagen einige Vertreter, die Pressefreiheit eingeschränkt, in dem man die Berichterstattung über ein bestimmtes Thema verbietet.

Das finde ich auch richtig so.

Ich wollte nur sagen, dass die Pressefreiheit gar nicht so frei ist, wie man sie jetzt gerade einschätzt.

Weshalb macht denn die Presse das? Dass sie dann berichtet, was da geplant ist? Macht sie das, um die Bevölkerung zu informieren, weil sie meint, dass das die Bevölkerung wissen sollte oder weil sie dann die besseren Auflagen bekommt? Das ist die Schwierigkeit.

Der Punkt ist ganz wichtig.

Das Stichwort Informationen bei der Presse über die Einführung von Sicherheitstechnologien. Wie würden Sie das beurteilen? Ist es ausreichend die Presse zu informieren? Vertrauen Sie der Presse?

War es jetzt Konsens, dass wir die Presse überhaupt informieren müssen?

Es können ja durchaus mal Dinge so gemacht werden. Nicht jede Strategie muss öffentlich sein. Das ist ja nur ein Mittel, was die Polizei sich nimmt und dann Grundrechte einschränkt, kann es doch, ohne dass es großartig diskutiert wird oder bekannt gemacht werden muss, angewendet werden.

Sie haben da auch das richtige Wort benutzt. Solange die Grundrechte nicht beeinträchtigt werden, braucht die Presse solche Sachen nicht veröffentlichen.

Aber wer überwacht das?

Deshalb sag ich ja auch, dass wir ein demokratischer Staat sind. Und ich hoffe, dass die Kommissionen im Bundestag auch damit vertraut gemacht werden und die müssen uns dann gegenüber schon glaubhaft sein. Davon geh ich eigentlich aus. Ich finde, dass die Pressefreiheit da nicht eingeschränkt ist.

Nun werden ja Gesetze und Verordnungen irgendwann veröffentlicht, wenn sie erlassen worden sind. Würden Sie sagen, dass es dann auch Geheimgesetze geben müsste, zum Beispiel, damit die Polizei Befugnisse hat, von denen nicht sofort jeder weiß, damit man auch keine Gegenmaßnahmen unternehmen kann?

Ich glaub, dass es manchmal ganz gut ist, wenn man so was nicht weiß.

Das sieht man ja bei diesem Militärausschuss, der geheim tagt. In dem Moment, wo das alles um meine Sicherheit geht, in einem demokratischen Staat, bin ich der Meinung, dass wir das zulassen müssen.

Ich bin eigentlich grundsätzlich dafür, dass eigentlich Dinge erstmal veröffentlicht werden sollten. Aber wo es natürlich um so etwas geht, gebe ich Ihnen auch Recht, da muss man auch Einschränkungen machen, aber, wenn meine Freiheit eingeschränkt wird, kann man auch andere Freiheiten einschränken, wie zum Beispiel die Meinungs- oder Pressefreiheit, so dass man da eben auch Einschränkungen macht. Bloß ist da wieder das Problem der Überwachung. Wie weit gehen solche geheimen Abkommen? Und ich glaube, dass es das jetzt auch schon gibt und dass wir wahrscheinlich nur noch nichts davon mitbekommen haben.

Aber manchmal sind wir auch blauäugig.

Ich glaube, aber, wenn man alles wüsste, was da passiert...

Was wir nicht wissen, das kann uns keine Sorgen machen.

Kleines Beispiel. Vor paar Monaten gab es die Diskussion zur Onlinedurchsuchung von PCs. Und da ist jetzt im Nachhinein dieser ganzen Diskussion ist plötzlich aufgetaucht, dass es von Otto Schily eine Anordnung gab, die es dem BKA erlaubt solche Durchsuchungen von PCs online durchzuführen. Es gibt dafür keinerlei gesetzliche Grundlage, zumindest

keine offizielle gesetzliche Grundlage. Schily hat damals ein Papier unterzeichnet, dass in der Lesart einiger Leute das BKA dazu ermächtigt. Das ist eine Bestimmung, die gar nicht öffentlich war. Das ist jetzt erst im Nachhinein aufgetaucht, selbst Schäuble wusste davon nichts, dass Schily das mal unterschrieben hat. Das BKA hat solche Onlinedurchsuchung durchgeführt, ohne dass die Öffentlichkeit in irgendeiner Form davon informiert war. Es war in diesem Fall sogar so, dass nicht mal einschlägige politische Instanzen darüber informiert waren. Das ist jetzt nur so ein kleines Beispiel, wo Befugnisse erlassen werden, die aber geheim sind und wo dann hinterher in der Öffentlichkeit ein großes Erstaunen entsteht, warum denn überhaupt solche Befugnisse existieren. In diesem Fall hat sich dann auch noch die Frage gestellt, ob diese Befugnis überhaupt gesetzeskonform ist. Aber nur als Beispiel wir nehmen an, dass sie gesetzeskonform, wäre das denn so was, wo dann Jahre später plötzlich klar wird, dass es da ein Gesetz aufgrund einer Befugnis gibt, aufgrund derer das BKA schon längst reagiert. Ist so was für Sicherheitstechnologien sinnvoll, um den Verbrechern keine Möglichkeit in die Hand zu geben sich dagegen zu schützen?

So wie Sie uns das jetzt erklären, wenn Schily noch seinen Posten hätte, wäre das ein Grund ihn zu entlassen. Indem Moment, wo er was gemacht hat, das nicht mit demokratischen Überlegungen einhergeht, dann ist das frevelhaft.

Wenn es dem Gesetz widerspricht ja, aber ansonsten...

Das ist ganz klar, die einen Politiker sagen, dass es dafür keine Gesetzesgrundlage gibt, Schäuble sagt, dass er schon eine gesetzliche Grundlage sieht, hat es aber erst mal auf Eis gelegt. Das ist zurzeit eine große politische Diskussion, offensichtlich kann man also das Gesetz auch interpretieren. Aber das ist jetzt gar nicht unser Thema. Es ging ja eher darum, welche Regulierungen, welche Begrenzungen bei der Einführung von Sicherheitstechnologien eingehalten werden sollten. Und zwei sind schon gesagt worden. Wer überprüft denn das ganze? Wer hat denn da sein Auge drauf, dass bei der Einführung alles mit rechtsstaatlichen Mittel zu geht?

Ich meine eigentlich, dass das bei uns in Deutschland recht gut läuft. Und man weiß ja auch gar nicht wodurch dass mit Schily jetzt wieder bekannt geworden ist, dass Schily da unterschrieben hat. Wollt sich da einer groß tun? Ist das eine politische Überlegung? Das ist es ja immer, den wischen wir noch mal ganz zum Schluss einen aus. Schily hat es ja gemacht, weil er meinte, dass er damit etwas erreichen würde.

Aber schon ist da irgendwo wieder was durchgesickert.

Und schon ist das was durchgesickert und jetzt ist die Frage, warum da etwas durchgesickert ist, weil derjenige, der das gesagt hat, dass es gegen die Rechtsstaatlichkeit ist und wollte damit Punkte machen. Das weiß man heute eben nicht. Da hat man Recht, wenn man sagt, dass das alles ein bisschen in Frage gestellt werden muss.

Und deshalb, wenn da ein Mensch dabei ist, können sie keine Hand ins Feuer legen, gar nichts und das ist das gefährliche dabei.

Also, ich finde schon, dass es auf jeden Fall sehr wichtig ist, dass auch die Bevölkerung darüber informiert wird, natürlich nicht über die Details, dennoch ist wichtig, dass die Bevölkerung weiß, dass es ein Sicherheitssystem gibt. Die Details muss natürlich die Firma,

die es macht und diejenigen Behörden für sich behalten, weil dann wieder die Gefahr, dass Kriminelle das missbrauchen. Welchen Nachteil hat es jetzt, wenn die Bevölkerung das weiß und die Bevölkerung das auch noch überwacht hat? Ich denke, dass gerade in solchen Sicherheitskreisen, auch gerade mit den Handys mehr gemacht wird, als sie letztendlich dürfen. Wenn es allerdings zu gerichtlichen Sachen kommt, werden sie immer wieder das Problem haben, wie man das rechtskräftig machen kann. Das Problem ist einfach, dass man diese Instanzen ja nicht überwachen kann, weil die nur dem Bundesrat oder dem Bundestag Rechenschaft schuldig sind und selbst so ein Geheimdienst das nicht überwachen kann. Gerade bei so was wie Sicherheitstechnologien sollte die Bevölkerung informiert sein und das auch ein wenig überwachen können.

Noch mal zur Sicherheit. Wir waren jetzt auf den Kanalinseln Jersey und die anderen kleinen, da sind wir einen Tag rumgelaufen und das fanden wir ganz normal. Und dann hatten wir eine Führung und dort habe sie uns dann auch auf die Kameras aufmerksam gemacht. Das ist ja unvorstellbar, wie viele Kameras die da

Da wird man doch ganz schnell nervös, oder nicht?

Nein, gar nicht. Wir fanden das nur interessant. Einmal dachte ich denn da, hoffentlich sieht mich denn auch einer, wenn da was passieren sollte. Man gewöhnt sich auch an so was und man fragt sich natürlich, warum diese Inseln diese Sicherheit brauchen. Das ist ja eigentlich ganz einfach Kriminelle, die von außen kommen zu fassen, weil ja alle mit den Flugzeugen oder Fähren nur dorthin kommen. Aber die haben das und somit konnten wir auch die Gefängnisse besichtigen.

Also ich könnte mir auch vorstellen, dass es wahrscheinlich auch damit zusammenhängt, dass Sie das vielleicht noch kennen, dass das also früher noch war, dass der Staat sehr stark überwacht hat und das da vielleicht noch so ein bisschen Misstrauen vorhanden ist. Ich könnte mir vielleicht vorstellen, dass es einen in irgendeiner Zeit nicht mehr stören wird, wenn überall Kameras angebracht sind. Und wenn man seinen Ausweis mit den biometrischen Daten benutzt und ob es jetzt Sinn macht oder nicht. Das wird alles nur eine Gewöhnungssache sein.

Haben Sie eigentlich alle Ihren Personalausweis mit?

Ja.

Ich habe meinen schon 40 Jahre nicht dabei. Ich habe den nie dabei. Und mein Sohn hat ihn immer dabei.

Es besteht keine Ausweispflicht in Deutschland. Sie müssen den auch nicht mit sich tragen.

Also, wenn Sie mich jetzt fragen würden wer ich bin, hätte ich noch nicht mal eine Kreditkarte oder so dabei. Das müssten Sie dann einfach so glauben.

Ich habe ihn jetzt eigentlich auch mitgenommen, weil ich dachte, dass danach gefragt wird.

Nein.

Aber es hätte ja sein können.

Sagen wir mal so, als es los ging, habe ich es deshalb nicht mitgenommen, weil ich meinen Führerschein dabei habe und der ist von 1956. Und den können sie heute nicht mehr lesen. Und den habe ich zu Hause, davon habe ich nur eine Kopie im Auto. Und wenn man auf nette Polizisten trifft, dann gilt es, ob sie damit was machen können. Und so war es mit meinem ersten Ausweis auch. Der wurde immer so zerknüllt. Und da habe ich mich dran gewöhnt. Und jetzt vielleicht genau das, wo Ihre Frag hinzielt. Ich fühle mich frei. Die Idee ihn nicht mitzunehmen hat sich verändert. Heute haben wir den freien Staat, da brauch ich es nicht. Ich nehme ihn auch mit, falls mal was passiert.

Wo muss ich mich melden? Denn, wenn Sie irgendwo auf der Straße umgefallen sind, muss man das ja wissen.

Ich habe da auch Diskussionen mit meiner Frau, die hat immer so was dabei. Ich nie. Wenn ich mich mal längere Zeit nicht bei meiner Frau gemeldet habe, fragt sie sich, was los ist.

Ich möchte so ganz langsam zum Schluss kommen, um Ihre Zeit auch nicht zu sehr zu strapazieren. Erste von zwei Schlussfragen. Hat die heutige Veranstaltung Ihre Sicht auf Sicherheitstechnologien und auch Privatsphäre in irgendeiner Form verändert? Sehen Sie eventuell das eine oder andere kritischer? Sind Sie von dem einen oder anderen irgendwie interessierter?

Also das Interessante war, dass wir vorhin zum Ende des Fragebogens die Frage auch schon mal hatten, ob sich die Meinung verändert hat. Nach dem Fragebogen war ich der Meinung nein. Ist jetzt durch dein Austausch eigentlich gleich geblieben. Aber ich habe gemerkt, dass ich in einigen Punkten, wie wahrscheinlich auch viele andere Leute auch, eine Meinung habe und die noch nicht gut genug überprüft habe. Da sind mir jetzt einige Punkte aufgefallen, wo ich mir gedacht habe, dass das unschlüssig und noch nicht ganz logisch ist. Das passt irgendwie nicht zusammen. Das ist wahrscheinlich auch einfach normal, dass man auf einen Punkt stößt, dass das alles nicht mehr zusammenpasst. Vielleicht muss ich da einfach noch mal ein bisschen drüber nachdenken, weil es ein sehr komplexes und schwieriges Thema ist. Ich denke auch, dass sich das im Laufe des Lebens einfach ändern wird, je nachdem in was für einer Situation man sich gerade befindet.

Sicherlich sind einige Sachen dabei, die man sich noch mal durch den Kopf gehen lässt, worüber man sich vorher keine Gedanken gemacht hat. Es sind doch schon aus dieser Diskussion Anregungen hervorgegangen, über die man vielleicht noch mal genauer nachdenken sollte. Oder auch die Dinge, in denen man sich überhaupt nicht auskennt, dass man sich da noch mal die Texte zum Durchlesen nimmt. Und da sind schon einige Überlegungen, die man jetzt machen müsste. Man könnte auch sagen, da habe ich jetzt drüber weggeguckt, aber das sollte man sich noch mal überlegen.

Ich hatte ja schon zum Anfang gesagt, dass ich so ein relativ egales Meinungsbild hatte. Ich hatte es eben nicht als Problem gesehen, sondern einfach darauf vertraut, wie es ist. Es hat sich jetzt nicht doll verändert, aber so ein paar Sachen, die sehr kritisch waren, habe ich natürlich auch gewürdigt. Und es hat vielleicht auch ein bisschen mehr Wissen verschaffen.

Bei mir war es so, das ich von vorn herein schon Einiges in Science-Fiction-Büchern gelesen hatte, was eben in diese Richtung geht. Und wo man halt doch merkt, dass es sich alles sehr angenähert hat. Dass Sachen, die in den achtziger Jahren geschrieben wurden, mittlerweile doch schon eingetreten sind. Das war auf jeden Fall ein Aha-Effekt. Durch diese Science-

Fiction-Sachen bin ich eher kritischer den Überwachungssachen gegenüber eingestellt. Ich finde es auch gut, dass hier verschiedene Generationen an einem Tisch sitzen und auch so verschiedenen Meinungen aus den verschiedenen Sichtweisen, die natürlich auch vom Alter abhängen zu sehen. Ich fand auch, dass die Diskussion deutlich mehr gebracht hat als das davor mit dem Vortrag und dem Fragebogen.

Meine Meinung hat sich nicht geändert, ich hoffe auch, dass ich meine Meinung nicht ändern muss. Man hat jetzt Wissen durch diese Gespräche erlangt und darüber werde ich auch nachdenken, aber das ist jetzt nicht so, dass ich mich meiner Meinung nach ändern müsste.

Dann haben Sie jetzt noch die Möglichkeit letzte große Worte zu sagen, die dann später transkribiert und ausgewertet werden. Wer möchte?

Allein, dass es so ein Forum gibt, spricht ja schon wieder dafür, dass es Institutionen gibt, die ein Auge darauf haben. Der Staat funktioniert ja ganz gut, weil wir ja selbst so eine Instanz sind. Immerhin wird es auch noch gewürdigt, dass es eine Diskussion wert ist.

Ich finde es auch sehr schön, dass es so was gibt und das man so was machen kann. Es war mir wichtig herzukommen, sogar wichtiger als die Kieler Woche. Von daher finde ich das gut, dass man sich daran beteiligen kann und dass man sich daran beteiligt.

Wir wissen ja, dass Sie eine gute Institution sind, aber man kann das ja auch umdrehen. Wir können auch sagen, dass die uns einfach mal fragen wollen, wie das so bei uns aussieht. Wenn das jetzt andersrum wäre, was machen wir dann? Dann vertrauen wir Ihnen voll. Oder?

Deswegen versuchen wir möglichst viel Anonymität zu gewährleisten.

Wir gehen davon aus, dass Sie sagen, dass Sie in Ordnung sind.

Natürlich müssen sie uns letztlich vertrauen.

Nicht, das das von der anderen Seite ist.

Group 3

Im Grunde wiederholt sich das Ganze. Ich finde auch, dass das alles manipuliert werden kann und das ist doch die Gefahr. Und deshalb würde mir das mit der Verwechslung auch nicht gefallen.

Ich sehe auch die Punkte, die Sie genannt haben, auf der anderen Seite die Verwechslung, die ja völlig unschuldig passieren kann.

Ja, ja, davor habe ich ja Angst.

Dann noch die Verwechslung, die gezielt passieren kann. Da ich politisch ein wenig aktiv bin, habe ich da auch die eine oder andere Einstellung, die anderen Personen nicht gefallen könnte

und ich möchte da nicht ins Visier geraten, solange ich nicht kriminell bin, sondern ich möchte meine demokratischen Rechte frei wahrnehmen können ohne, dass da zum Beispiel mein Profil registriert wird. Das ist der eine Punkt. Meine Privatsphäre empfinde ich durchaus auch in der Öffentlichkeit so, wenn es zum Beispiel sehr warm ist und ich ein bisschen weniger an habe, natürlich dennoch normal bekleidet, dann möchte ich nicht, wie es auch Beispiele gegeben hat, dass bei Kameras hinter denen Männer sitzen dann doch mal ranzoomen und sich ein Vergnügen daraus machen mich zu beobachten. Zum Beispiel auf dem Bahnhof. Da braucht ...Sagen Sie nicht, dass so was nicht passiert...

Ich habe jetzt nur gedacht, dass es mir egal ist, ob die am Bahnhof heranzoomen oder nicht.

Ja, das ist schön. Mir nicht.

Ich sitze im Zug ja auch irgendwelchen unbekannten gegenüber.

Ja, aber die suchen Sie ja aus.

Nein, die kann ich mir nicht aussuchen.

Ich kann ja ein paar Schritte weitergehen

Man kann ja auch einfach aufstehen und sich woanders hinsetzen.

Meine Privatsphäre beschränkt sich nicht nur auf mein zu Hause, auch in der Öffentlichkeit bin ich eine Person. Da möchte ich mir nicht alles gefallen lassen, also alles, was eventuell passieren könnte. Und auf einer anderen Ebene finde ich dieses ganz trügerische Sicherheitsgefühl, zum Beispiel an öffentlichen Plätzen, die mit Kameras überwacht werden. Ich kenne das selber auch, dass ich mich ein bisschen sicherer fühle, aber was für eine Sicherheit ist es dann, wenn dahinter gar keiner sitzt? Wenn mir jemand etwas tut, dann passiert gar nichts. Das einzige, was denn passieren könnte, ist, dass der Täter vielleicht gefasst werden könnte. Ich bin da aber nicht wirklich sicher, aber ich fühle mich eventuell so. Und das allgemeine Sicherheitsgefühl durch die Hochtechnologie vor Terrorismus, die wir einsetzen, das finde ich, ist immer noch das Gefährlichste, dass man da ganz viel Geld und Energie reinsteckt und sich nicht fragt, ob auf dieser Welt das Leben so ist, wie es sein sollte, oder nicht. Muss ich vielleicht mein Leben noch ein bisschen ändern, damit ich mein Leben noch effektiver gegenüber anderen abschotte? Das sind für mich wichtige Fragen.

Wechseln wir mal so ein bisschen den Fokus. Versuchen sie sich mal zu überlegen, unter welchen Umständen Ihrer Ansicht nach die Sicherheit wichtiger als die Privatsphäre ist. Also, wo man sozusagen Eingriffe in die Privatsphäre rechtfertigen kann, um die Sicherheit zu fördern. Und in welchen Situationen die Sicherheit einfach hinter der Privatsphäre zurückstecken muss, ganz abstrakt. Ist es klar geworden, was ich damit meine? Versuchen Sie sich mal eine Situation vorzustellen, in der das eine das andere überwiegt, also im Bereich der Sicherheit gegenüber der Privatsphäre, aber auch , wo ist die Privatsphäre auf jeden Fall höher zu bewerten. Fallen Ihnen da irgendwelche Situationen ein?

Also, die Flughafenkontrollen finde ich schon wichtig. Und was mich stören würde, das ist natürlich, wenn jetzt zum Beispiel komplett alle Telefone abgehört werden, um dann vielleicht einen Verdächtigten zu finden.

Da wäre Ihnen die Privatsphäre wichtiger als die Sicherheit?

Ja.

Gut.

Oder mit diesem E-call, da sollte auch wirklich gezielt und nicht per Zufall da jemanden überwachen. Bei Unfällen und Geschwindigkeitsüberschreitungen finde ich das übertrieben.

Das ist natürlich schwierig. Eine Situation, in der vielleicht die Sicherheit überwiegen könnte, wäre, wenn ein Kind, ein noch relativ junges Kind, verschwunden ist und man weiß, dass es ein Handy dabei hat. Das ist zwar auch ein Eingriff in die Privatsphäre, aber, wenn da Anhaltspunkte sind, dass das Kind in Gefahr sein könnte oder es ein Mensch ist, der nicht im Vollbesitz seiner geistigen Kräfte ist, wenn das sicher ist, auch wenn es geistig behinderte Menschen sind, die sich alleine nicht zurecht finden, dann kann in den Situationen die Sicherheit überwiegen.

Zum Beispiel diese Speicheltests, die ja oft bei Männern gemacht werden, wenn ein Kind ermordet wurde oder so. Wenn sich dann in der Umgebung alle freiwillig untersuchen lassen wollen. Und sobald es dann jemand nicht tut, ist er verdächtig. Das ist natürlich auch schwierig. Aber in dem Fall, wenn ein Kind oder eine andere Person umgebracht worden ist, finde ich, dass jeder Mann mit einem gesunden Menschenverstand sagen wird, dass er sich da testen lassen will. Das halte ich dann doch schon für besser, dass wenn ich nichts auf dem Kerbholz habe, da dann auch hingehere, um mich untersuchen zu lassen. Da ist zwar vielleicht in meine Privatsphäre eingegriffen worden, aber das sehe ich nicht so. Da finde ich es schon besser die Karten offen zu legen.

Aber wenn Sie eine Erbkrankheit haben, von der Ihr Arbeitgeber nichts weiß, also so eine, bei der es ziemlich sicher ist, dass Sie irgendwann arbeitsunfähig sind und diese Daten können dann damit erhoben werden.

Ist das nicht soweit geschützt, dass der Arbeitgeber das nicht erfährt?

Theoretisch ja.

Wenn ich denke, dass ich wegen der Wahrheitsfindung dorthin gehe, dass das schon richtig ist. Die Daten dürfen ja nicht weitergegeben werden, oder? Und wenn ich so einen schlechten Gesundheitszustand habe oder die Fakten in meiner Krankenakte stehen, dann ist doch die Frage, ob ich das sowieso nicht bekannt muss.

Wenn Sie nur wissen, dass Sie in 7 bis 15 Jahren vermutlich schwer erkrankt sind und bis dahin arbeitsfähig sind, glaube ich nicht, dass Sie das bekannt geben müssen. Bis jetzt haben Sie da die Garantie, dass Sie nichts sagen müssen. Und Ihr Arbeitnehmer muss dann gegebenenfalls für Sie zahlen, auch wenn der das natürlich nicht will. Das ist für mich der einzige Grund, warum ich nicht dafür bin, dass für jeden Menschen sowieso eine Gen-Datei angelegt wird. Das ist genau dieser Verbrechensgrund. Gerade so bei Mord und Vergewaltigung, wo ich sage, dass das eine sehr hohe Menschenrechtsverletzung ist, wäre ich bereit ziemlich weit zu gehen. Aber andererseits ist da dieser Missbrauchsgrund. Ich habe nicht das Vertrauen, dass es nicht irgendwo eine Firma gibt, die einen solchen Fall zum Beispiel ausnutzen würde.

Nein, ich auch nicht..

Das Vertrauen habe ich nicht In die Gesetze ja.

Aber dann müssten wir ja alles in Zweifel stellen, weil es überall irgendwelche Lücken gibt, die die Kriminellen ausnutzen. Und dann wäre es auch günstig sich über Sicherheitstechnologien zu streiten, weil ich sie je gerade wegen dieses Grundes abschaffen möchte und die anderen dann aber die Überhand haben.

Gibt es dann noch andere Situationen, in denen Sie Schutz von hilfsbedürftigen Personen, wenn man da noch mal ein bisschen weiter in den Alltag geht, öffentliche Verkehrsmittel, die Richtung, gibt es da irgendwo Situationen, in denen Sie sagen würden, dass das eine das andere überbieten muss. Wollen wir versuchen uns noch andere Szenarien zu überlegen?

Also ich persönlich habe auch dieses spontanen Eindruck, dass man bei Flugzeugen wirklich besonderes aufpassen muss. Lass uns noch mal 5 Jahre warten, dann geht das erste Schiff hoch. Dann sitzen wir hier alle und denken, dass nicht mehr sicher ist. In London sind die ersten Busse und U-Bahnen hochgegangen. Bei Flugzeugen und bei U-Bahnen müssen wir also wirklich aufpassen. Das zeigt doch im Grunde die Reaktionen, die wir haben. Wir reagieren auf das, was passiert. Und irgendwann haben sie alle öffentlichen Verkehrsmittel durch. Was sagen wir denn dann? Was weiß ich, wann dann noch kommt? Dann kommen vielleicht Autobahnen. Diese Menschen sind, wie wir schon sagten, hochintelligent und sehr gut ausgebildet. Das bleibt nicht bei Flugzeugen. Es kann sein, dass in den nächsten 10 Jahren kein einziges Flugzeug angegriffen wird, aber wir haben bestens abgesicherte Flughäfen. Ich habe auch immer das Gefühl, dass ich dort richtig sicher bin. Ich könnte es nicht überall so sagen.

Na ja, die Schiffe sind ja auch schon abgesichert.

Aber nicht in den Maßen.

Nicht in dem Maße, aber sie sind nicht mehr frei zugänglich. Vor drei Jahren war es doch noch so. Und das fängt überall so an.

Das ist ja auch so mit den Zügen. Gerade hatten wir das hier in Kiel mit den sogenannten Kofferbomben. Wo fühlt man sich dann noch sicher? Ist es denn wirklich eine größere Sicherheit, wenn man da mit biometrischen Daten rangeht Ich laufe eigentlich ständig mit einem Rucksack rum, das ist dann sozusagen meine Handtasche. Wenn ich denn da einfach mal nach Hause fahren möchte, um meine Mutter zu besuchen, dann muss ich mich erst durchleuchten lassen oder überlegen den Rucksack zu Hause zu lassen? Wenn ich fliege, darf ich schon Kosmetika nicht mehr mitnehmen. Wo sind da die Grenzen? Abgewogen an diesem, können wir da eigentlich die erträumte Sicherheit erreichen?

Weil Sie das auch schon angesprochen haben, kommen wir dann dazu, wer eigentlich mit in der Entscheidung über den Einsatz und die Entwicklung neuer Sicherheitstechnologien daran beteiligt sein sollte.

Das Parlament.

Ok.

Früher haben wir es gewählt und die sollten auch ihre Aufgabe ernsthaft ausführen.

Ist es Einstimmigkeit?

Beteiligt? Natürlich auch der Bürger.

Können Sie sich da irgendwelche Formen vorstellen?

Also, ganz gering wollen wir ja schon was sagen. Aber was letztlich in Gesetze oder Verordnungen gegossen werden muss, ist das Parlament.

Das ist ja der Einsatz. Aber auch bei der Forschungsentwicklung. Ich hatte ja bewusst zwei Punkte angesprochen, einmal den Einsatz und dann aber auch die Entwicklung. Soll es da Bestimmungen geben? ...Soll man Forschungsunternehmen freie Wahl lassen? Oder sollte da auch ein Mitbestimmungselement eine Rolle spielen?

Also ich finde, dass man der Forschung freien Lauf geben sollte. Aber, was dann umgesetzt wird, das sollte man kontrollieren.

Sie hatten das irgendwie angesprochen. Das eine ist freie Handhabung und das andere ist als ob Ihnen jemand Geld gibt. Als ob man da öffentlich Steuermittel dazu gibt. Ob man da eher sagt, dass die schon wissen, was sie tun oder ob man das tatsächlich von Beteiligungsverfahren abhängig macht. Sei es durch Parlamentarier oder so was wie hier, sei es eine Volksabstimmung gegen die ich mich wehre. Aber da denke ich schon, dass die Vergabe öffentlicher Mittel für die Forschung in diesem Bereich Auflagen bekommen sollte.

Die gemacht werden von?

Von den jeweiligen Parlamenten. Und die zumindest eine ganz starke Transparenz herstellen müssen. Also, woran wird geforscht? Wo geht es hin? Was kann damit passieren?

Ganz transparent, damit die Terroristen genau Bescheid wissen.

Ja, das ist der Nachteil.

Also ich möchte schon gerne wissen, ohne dass ich ein Terrorist bin, was mit meinen Steuergeldern passiert. Und ich glaube ehrlich gesagt auch nicht, dass irgendein Staat, auch nicht unser, die Chance hat, ohne ausgeforscht zu werden so etwas zu erforschen. Die Chance gibt es nicht, vielleicht mal für einen Monat. Denn auch gerade in diesem Bereich wird es immer Spionage geben.

Ja sicher hat es die noch gegeben, als das Internet noch nicht für die Allgemeinheit zugänglich gewesen war, und es nur ein wissenschaftliches Internet gab. Da gab es das schon.

Ist das Parlament ausreichend, sowohl bei der Entscheidung über was geforscht wird, als auch bei der Entscheidung, was umgesetzt wird? Die einen sprachen ja zum Beispiel von einer Volksabstimmung.

Wenn ich mir nur das Volk mit den unterschiedlichen Begabungen ansehe, und wenn ich so von den Wahlen höre und mir die Leute ansehe und diese Leute insgesamt bestimmen nun, wer über uns bestimmen soll, dann weiß ich das nicht. Die wählen doch nicht nach dem, was die Leute von den verschiedenen Parteien gemacht haben, sondern nur danach, wer mal etwas ganz tolles gesagt hat oder wo ein Schlagwort gefallen ist. Die wenigsten machen sich doch ernsthaft Gedanken oder gucken sich die Programme der Parteien an. Und da habe ich schon meine Bedenken, wenn wieder neue Wahlen stattfinden, was dann dabei herauskommt. Weil das doch irgendwie nicht so ganz Intelligenz mäßig hoch angesiedelt ist. Die wählen alle uns haben alle dieselbe Stimme, das finde ich bedenklich.

Und wollen Sie Wahlen abschaffen?

Das kann ich nicht. Was soll ich denn machen. Ich wollte nur sagen, dass da nicht viel bei heraus kommt.

Ich kann Ihnen ein paar Stichwörter liefern. Die eine Möglichkeit war die Befragung der Bevölkerung, also eine Volksbefragung, die andere Möglichkeit wären Bürgerrechtsorganisationen, Sicherheitstechnologien oder Politiker.

Also, wenn ich Parlament sage, meine ich, dass die da schon ihre speziellen Leute haben, die etwas davon verstehen. Wenn ich sage, dass das Volk entscheiden soll, geht das gar nicht, weil der einzelne das nicht versteht. Das habe ich impliziert, wenn ich Parlament sage, dass dann Experten da sein und es ausbreiten müssen. Und in sofern...

Experten welcher couleur?

Wissenschaftlich. Also nicht nach Partei.

Aber es geht ja auch um Industrie oder Bürgerrechts- und Menschenrechtsvereinigungen.

Die sind manchmal auch sehr unterschiedlicher Meinung.

In einem transparenten Verfahren müssten sie alle zu Wort kommen. Die Industrie wird ohnehin zu Wort kommen, weil sie ihr Interesse artikulieren wird, weil es durch einen Antrag, da in der Regel Fördergelder beantragt werden müssen, werden ihre Möglichkeit haben die Vorteile darzustellen. Und das tun sie ja auch. Und in einem transparenten Verfahren muss es für alle möglich sein sich zu äußern.

Und durch diese Äußerung, das man die sammelt und das danach die Regierung entscheidet, wie sie als nächstes vorgeht. Denn ich denke doch, dass die Grundlagen haben und nicht einfach nach ihren Kriterien entscheiden. Die berufen sich doch auf Ausschüsse und dann finde ich das schon in Ordnung.

Ich finde diesen Punkt je mehr man offenlegt, dass man sich dadurch noch leichter angreifbar macht, ist natürlich jetzt für die Gegenseite. Das ist einerseits völlig richtig, aber andererseits ist das auch ein Argument mit dem man alle Transparenz ausheben kann. Und deswegen empfinde ich das als so gefährlich.

Ja, da ist immer die Frage, wie groß mein Vertrauen zu den Leuten, die im Bundestag sind. Wenn ich ein großes Vertrauen hätte, dann würde ich sagen, dass das nicht offengelegt werden sollte, weil die dafür gerade stehen. Wenn ich mein Vertrauen in die hätte, aber das ist genauso wie Sicherheit und Privatsphäre.

Es ist ja die Aufgabe des Volkes die Regierung zu kontrollieren. Diese Aufgabe möchte ich auch gerne weiterhin wahrnehmen. Ich möchte weiterhin die Vertreterinnen und Vertreter des Volkes kontrollieren.

Ja, das sind doch die Vertreter des Volkes. Das Volk ist ja zu groß. Es kann ja nicht jeder von uns hingehen und sagen, was die Regierung da gerade machen soll.

Aber Sie haben doch Ihren Ansprechpartner, Ihren Abgeordneten Ihres Wahlkreises. DA könnte Sie doch theoretisch...

...dieses Parlament wählen.

Dann geht es um das Parlament. Jeder einzelne kann ja zur...

Wir haben es auch schon angesprochen. Ich möchte es nur noch mal abklopfen, ob da vielleicht noch Ideen sind. Haben Sie irgendwelche Überlegungen, Ideen oder Vorstellungen, was zusätzlich zu den momentanen Möglichkeiten Sicherheitstechnologien umzusetzen und zu entwickeln, ob es da noch Vorschläge Ihrerseits gibt, wie man zum Beispiel Transparenzanforderungen, wie sie gerade eben gestellt wurden wie man sicher stellen kann, dass das sicher umgesetzt wird. Haben Sie da irgendwelche Ideen, wie man das eventuell machen könnte? Wir haben jetzt auch schon über bestimmte Verfahren diskutiert. Fällt Ihnen noch was ein, was es da für Verbesserungen geben könnte? Aus Ihrer ganz persönlichen Sicht.

Das Thema im Schulunterricht. Auch wenn mich diese Themen alle interessieren, war ich nicht auf dem Stand bevor es zu dem Fragebogen kam. Und ich denke, dass Kinder und Heranwachsende schon wissen sollten, was alles möglich ist und darüber diskutieren sollten. Genau über das, worüber wir reden. Wie ist die Abwägung zwischen Sicherheit und Privatsphäre? Dass sie sich eine Meinung bilden. Und ich halte es für wichtig, das schon in der Schule zu machen. Heutzutage ist ja auch häufig so, dass das was die Kinder in der Schule machen, häufig in die Familie hineingetragen wird. Und das wäre positiv. Ich denke, dass das ein Ort ist, an dem so was passieren sollte.

Da kann ich nur zustimmen. Das finde ich in Ordnung.

Jetzt machen wir noch mal einen kurzen inhaltlichen Sprung. Ich mach jetzt einfach noch mal eine Runde. Hat diese heutige Veranstaltung bei Ihnen eine Veränderung in der Haltung hinsichtlich der Sicherheitstechnologie und der Privatsphäre bewirkt? Hat sich da irgendwas verändert? Und wenn ja, in welcher Weise?

Eigentlich nicht besonders viel. Ich habe immer gedacht, so viel wie nötig und so wenig wie möglich. Und das ist auch jetzt noch meine Meinung.

Das ist bei mir auch so. Von der Grundeinstellung hat sich bei mir nichts verändert.

Bei mir auch nicht. Die Frage war auch schon auf dem Fragebogen.

Die einzige Veränderung ist, dass ich mich ein bisschen mehr mit diesem Thema beschäftigt habe. Ich habe mir vorher nicht so richtig Gedanken darüber gemacht. Jetzt habe ich mal mit ein paar Leuten darüber gesprochen und dann wird einem das ganze Problem doch ein wenig bewusster. Aber meine grundsätzliche Meinung hat sich nicht geändert. Was nötig ist muss sein, aber nicht mehr.

Ich finde es ganz interessant, welche Technologien es gibt, weil ich mich vorher gar nicht mit dem Thema befasst habe. Ich habe so gewisse Grundregeln eingehalten, dass ich ab einer gewissen Uhrzeit nicht mehr auf die Straße gehe und dass ich von der Selbstverteidigung her auf der Mitte der Straße gehe, damit man die Angreifer gleich sehen kann. Aber solch eine richtige Angst habe ich nicht, weil mich das ein wenig geschult hat. Wenn dann jede Woche einer auf mich zuspringt, ich meine, dass ich das nicht mache, dann wird man damit vertraut und es macht einem so ein Anblick nicht mehr so viel Angst. Ich habe immer nur darüber nachgedacht, wie ich meine Privatsphäre schützen kann, aber über Technologien hatte ich bisher noch überhaupt nicht nachgedacht. Das ist mir auch noch nie so nahe gebracht worden, bis auf die Sicherheitsautomaten, wo man sich mit einer Karte das Geld zieht. Sonst fühlte ich mich eigentlich immer ziemlich sicher.

Hat sich das jetzt geändert?

Nein, hat sich auch nicht geändert. Ich denke, dass meine Einstellung, dass ich das schon irgendwie hinbekomme, ist besser als dass ich irgendwie verängstigt bin, weil man ja die Angst des Gegners spüren kann. Ich habe eigentlich keine Angst, nur wenn ich alleine zu Hause in meiner Wohnung bin. Was da auf einmal passieren kann. Ich hatte da einmal auf dem Balkon Handwerker und da hatte sich denn bei der Tür zu dem Balkon hin der Griff gelöst, und dann habe ich da eine Stange vorgemacht, eben weil ich alleine zu Hause war, habe ich die wichtigsten Sachen aus dem Raum herausgeholt und den Raum dann abgeschlossen. Und danach habe ich gut geschlafen. Da habe ich gar nicht so große Ängste gehabt.

Wir sind schon fast durch. Fällt Ihnen zu der Veranstaltung, zu dem Thema noch irgendwas ein, was Sie noch sagen wollen, was Ihnen wichtig erscheint, dass es unbedingt noch mal zum Thema gebracht werden sollte.

Nein, eigentlich nicht, aber ich fand die Veranstaltung gut für mich.

Ich würde es wichtiger finden die Ursachenforschung zu betreiben.

Ich denke, dass das ein finanzielles Problem ist, wie man an den vielen Arbeitslosen und wenig Geld sowie die vielen Ausländer, von denen es auch viele nette gibt, sehen kann. Das ist glaube ich die Grundsituation aus der ganzen Sachen entstanden sind. Denn ich meine, dass wir vorher nicht darunter gelitten haben. Wenn ich Geld habe und es mir gut geht, dann komme ich nicht auf irgendwelche Gedanken, dann bin ich zufrieden. Aber wenn ich wenig Geld habe, dann versuche ich doch irgendwie an mehr Geld heranzukommen. Da kann man sich nicht mit abfinden, wenn man arbeitsfähig ist und man nicht weiß, was man zu Hause machen soll und steht dann irgendwo mit anderen zusammen, das finde ich sehr, sehr schlimm für die Leute. Ich habe nicht an irgendwelchen Ecken gestanden, aber als ich in den Ruhestand gegangen bin, habe ich auch gar nicht daran gedacht und man musste sich da erst wieder was aufbauen. Dass da eine gewisse Unzufriedenheit entsteht, kann ich verstehen. Aber ich könnte

mir vorstellen, dass so was passieren kann, wenn einer aggressiver ist. Es darf natürlich nicht ausfallend werden.

Ich finde, dass es nicht wirklich etwas bringt immer mehr Technologien zu entwickeln. Man muss erst mal gucken, wo das herkommt und wie man das sonst anders machen könnte.

Ich finde die Veranstaltung als solche ganz gut, dass die EU so in die Länder eingreift und auch mal hört, was die Leute da zu sagen haben. Das finde ich als positivstes von allem.

Das finde ich auch. Und ich finde es auch klasse, dass es die ULD gibt.

Ich schließe mich den Worten meiner Vorgänger an.

Group 4

Wir haben jetzt 9 Fragen. Es geht jetzt nicht darum, das in die Tiefe zu beleuchten und einzelne Aspekte sehr detailliert zu diskutieren. Dazu haben wir wahrscheinlich nicht die Zeit. Weil bei 9 Fragen und 60 Minuten merkt man das schon so ein bisschen, sondern auch weitere Trends einfach weiter zu beleuchten, die in dem Fragebogen dann evtl. zu kurz gekommen sind und da Ihnen auch noch mal die Möglichkeit zu geben, sich dazu zu äußern. Der erste Bereich, den wir besprechen wollen oder wo wir an Ihrer Meinung interessiert sind, ist, was Sie allgemein über Sicherheitstechnologien und Privatsphäre denken. Das ist eigentlich so die Einstiegsfrage und das ist ja auch so ein bisschen ein Spannungsfeld. Zum einen halt Sicherheit oder das Streben oder das Bedürfnis der Bürger nach Sicherheit und zum anderen der Privatsphäre.

Welche Fragen zur Sicherheitstechnologie sind denn jetzt gemeint?

Also es geht allgemein in diesem Forschungsprogramm, wie ich schon sagte, eher um innere Sicherheit, das, was auch durch die Szenarien so abgedeckt wurde. Denn man kann ja ...

Also, das meiste von diesem, was in den Szenarien abgedeckt wurde, finde ich also absolut, hilf mir mal mit den Worten, ist bewiesen, dass es nichts taugt. Und von daher ist es für mich keine Sicherheit, sondern es ist also nachweisbar, dass beispielsweise Fingerabdrucksensoren nur nach noch Sekunden gefälscht werden könne. Es ist mehr als bewiesen, dass RFID-Chips in Reisepässen totaler Blödsinn sind und dass es halt nicht hilft, dass es nur eine Pseudosicherheit gibt und dass letztendlich gesehen, diejenigen, die man damit kriegen will, ganz andere Wege gehen.

Das denk ich auch. Uns wird eine Sicherheit vorgegaukelt auf der einen Seite, zugleich wird ein Bedrohungsszenario geschaffen. Du bist permanent bedroht und deshalb stehen hier all die Geräte, d. h. sind hier all diese Kameras und das erzeugt vielleicht auch das Bedürfnis nach neuen und weiteren Sicherheitstechnologien und ich weiß ja nicht, sind wir vielleicht auf dem Weg zum Überwachungsstaat? Ich weiß es nicht.

Das sind wir in meinen Augen auf jeden Fall, mehr als.

Ja ich sehe das auch so, äußerst kritisch.

Gewisse Politiker reden Gefahren herbei, bei den Protesten gegen diese Aktionen, werden dann ggf. noch irgendwelche Provokationen dazu aufgeföhren und dann wird gesagt, wir haben es doch gesagt.

So wie der G8-Gipfel.

Ja.

Sehr gutes Beispiel.

Man erfindet eine neue Sicherheitstechnologie, und wenn man dann mit dieser Sicherheitstechnologie dann neue Terroristen findet, sagt man, dass es nötig war, offenbar, und wenn man keine findet, dann sagt man, dass offenbar noch mehr Überwachung nötig ist. Weil wir niemand Neues gefunden haben.

Also kann mit jeder neuen Technologie, die kann genauso auch wieder zum Missbrauch genutzt werden.

Trotzdem stellt sich demnächst die Frage, wozu es denn Sinn macht. Wenn man jetzt gar nichts machen würde, finde ich allerdings, dass es irgendwie auch nicht ganz in Ordnung ist.

Das ist das Dilemma.

Wenn wir uns überlegen, woran wir schon gewöhnt sind. Ich merk dann im Fragebogen: Kameras, wo akzeptiere ich inzwischen alle, vor einem Jahr war das noch völlig befremdlich, in einem Supermarkt von einer Kamera angeguckt zu werden und plötzlich nimmt man sie kaum mehr wahr. In Australien und überall ist es üblich, auf jedem Busbahnhof kommt die Durchsage, „Melden Sie sofort liegen gebliebene Koffer usw.“. Zu Anfang denkt man „Oh je, Terror“ und nach einer Woche merkt man gar nichts mehr, man hört die nicht mal mehr, diese Durchsagen.

Oder auch, was diese Terrorismusgefahr angeht, bin ich mittlerweile auch total kritisch geworden, weil ich ehrlich gesagt nicht so viel Terroristen sehe, wie da immer vermutet werden. Also die, die wirklich Mist vorhaben, die kriegt man mit so was um Gottes Willen überhaupt nicht, weil die sind so gewieft, dass die nicht auffallen. Das hat sich ja gezeigt.

Ja, denn die, die Flugzeuge in die Luft jagen, die hat man vorher auch nicht gekannt.

Seit 2001 ein islamisch motivierter Versuch einen Terroranschlag zu begehen in Deutschland. Und der hat nicht mal geklappt, weil die Leute zu blöd waren, einen Zünder zu konstruieren.

Einmal zur Diskussion. Ich halte mich da jetzt extra zurück. Nicht weil ich da keine Meinung zu habe, sondern da wir einfach auch diese Gruppendiskussion einfach sich entwickeln lassen wollen. Und auch, wenn Sie mich dabei angucken, bin ich jetzt nicht in der Rechtfertigungsposition oder reagier extra nicht darauf, nicht weil ich keine Meinung dazu habe, sondern weil man jetzt natürlich innerhalb dieses Projektes

sozusagen die Meinung der Bürger haben möchte, einfach, ohne dass Sie von uns bewertet oder zustimmend oder negativ beurteilt wird, weil man einfach sagt, das ist ne Diskussion und wenn da einer jene und ne andere Meinung zu hat, soll das jetzt nicht sozusagen sagen, weil der Fachmann sozusagen dazu sagt, das ist so und so richtig, dass er sich dann da nicht ermutigt dazu fühlt, Stellung zu nehmen. Vielleicht sollen wir da einfach, weil wir auch schon, ja,

Sind Sie so gut und reißen mal ganz kurz an, welche zusätzlichen Fragen Sie noch haben. Das ich also entsprechend etwa auch reagieren kann, wann ich dazu Stellung nehme.

Das sind nur Fragen, die das Gespräch ein bisschen leiten sollen, auch wenn Sie zu einer Frage irgendwann später sagen, das ist mir aber noch mal wichtig, das ist nicht so, dass Sie da zu kurz kommen. Wir können jetzt aber, das hat auch schon so ein bisschen angeklungen, zu der zweiten Frage kommen. Vielleicht, was denken Sie zu diesen Szenarios, die Sie zugeschickt bekommen haben? Ist das realistisch, ist das völlig unrealistisch oder muss...

Ich halte das generell für realistisch, dass die Technologie geben das schon seit Jahren her. Gestern erst war ein sehr interessanter Artikel von einem japanischen Mädchen, das automatisch oder die Eltern bekommen automatisch ne SMS, wenn das Kind den Zugang zur U-Bahn passiert, ja, das war ja die Diskussion mit der Überwachung der Person. Man kann sich das also nicht auch bei Älteren vorstellen, dass man weiß, ah ha, die alten Eltern, Behinderte oder so was sind irgendwo in einer Situation, wo sie Probleme haben. Die Szenarien waren alle durchaus realistisch, im Grunde sind sie auch hier untertrieben, technisch ist schon viel mehr möglich. Und Überwachungen, die waren absolut harmlos.

Wobei ich sie schon absolut schockierend fand.

Also technisch ist das machbar, da gibt es gar keine Diskussion drüber.

Dass das technisch alles machbar ist, ist gar keine Frage, aber ...

..und die Diskussion sehe ich dahingehend auch die Fragestellung für die europäischen Behörden, einmal auszuloten, wie weit können wir eigentlich gehen. Was, wie weit ist der Bürger bereit zu akzeptieren. Sie haben meines Erachtens wird deutlich gesagt, wir haben uns schon an alles gewöhnt, völlig richtig. Wir haben uns an Kontrollen auf den Flughäfen gewöhnt und somit sukzessive auch diese Technologie weiter fortschreiten.

... sich mal ne kurze Weile, jetzt dürfen wir nur noch 100 ml Portionen mal mit ins Flugzeug nehmen. Ich bin der Auffassung, es sterben mehr Menschen an Thrombose, weil sie auf Flügen nichts mehr trinken, als Menschen an Flüssigsprennstoff in Flugzeugen sterben.

Vor allem war das mit dem Flüssigsprennstoff totaler Blödsinn. Da haben sich etliche Chemiker drüber ausgelassen, dass es eine Vielleichtmethode gibt, die dann mithilfe von Flüssigkeiten ein Flugzeug sprengen könnte und die würde erst mal Reaktionen an Bord des Flugzeuges erfordern, die so um und bei 6 Stunden dauern, bis man genug Material zusammen hat um das womöglich zu sprengen. Also totaler Blödsinn.

Zu dem Szenario mit dem Scanner auf den Flughäfen, nur weil wir bei dem Thema Flughäfen sind, ganz nette Anekdote. Ich bin gestern mal in die Schweiz geflogen. Schweiz deshalb, ist

auch noch außereuropäisch, Schengener Abkommen. Biometrischen Pass musste ich logischerweise vorlegen. Mein Personalausweis hätte gereicht, ich hab ihn halt, ja, aber bei der Flugzeugkontrolle wurde ich gebeten, doch mal mein Gepäck aufzumachen und ich hatte drei Pakete mit Papier drin. Jetzt frag ich mich, sind die Scanner wirklich so gut, um das zu identifizieren. Und das war nur ein Gastgeschenk.

Sagten Sie mit Papier.

Ja, da waren drei gebundene Pakete mit Papierschnipseln. Toll ne.

Das ist gefährlich.

Das ist äußerst gefährlich. Und das ist die subjektive Sicherheit, die vielleicht einigen suggeriert wird und die letzten Endes aber dazu führt, dass die Bürger so was ablehnen.

Diese Scanner, die Röntgengeräte, die können da wohl auch nur sehen, dass eine relativ große Masse eines relativ gleichmäßig dichten Materials Es ist auch schon in Großbritannien eine Person festgenommen worden, weil sie eine Portion Plumpudding dabei hatte, welches in der Dichte sehr ähnlich zu Semtex ist.

Wollte das anreißen,

Gerne,

weil die Auswertemethoden werden versucht immer wieder zu verfeinern. Aber letzten Endes dient es nicht dazu, eine erhöhte Sicherheit zu bringen.

Wir brauchen uns ja auch nicht einzubilden, wenn man jetzt ermittelt im Laufe der Zeit, dass eine Sicherheitsmaßnahme nicht notwendig ist oder nicht trägt, dass sie wieder zurückgefahren wird.

Nein.

Das ist genau der Punkt, auf den ich drauf hinaus wollte. Ich denke gerade weil erwiesen ist, diese ganzen Methoden hier eingebracht worden sind, einfach zu nichts führen. Gerade deswegen werden sie auf jeden Fall eingeführt, weil man es dem Großteil der Bevölkerung immer noch verkaufen kann als das hilft gegen alles, es hilft gegen pauschal gegen Kinderpornographie und überhaupt.

Vor allem wenn man es zurückfahren würde, müsste ja irgendwer zugeben, dass er sich geirrt hat.

Ja und es entstünde ein Vakuum des Unsicherheitsgefühls. Nicht.

Vielleicht noch mal, wir hatten ja jetzt die Diskussion sehr um die Sicherheitstechnologie. In den Szenarios wurden ja eigentlich auch Menschen beschrieben, wie sie damit umgehen. Da ist zum einen die etwas ältere Dame, in diesem Fall Karla hieß sie glaube ich, die ja sehr kritisch damit umgeht, als auch Peter, der ja sag ich mal diese Bedenken nicht jederzeit versteht. Stimmen Sie da mit den Szenarios auch so überein, dass auch diese Stimmung in der Bevölkerung so ist?

Ich denke es gibt alles, ich stelle an mir fest, meine Einstellung hat sich wahnsinnig gewandelt. So vor 10 Jahren hätte ich vielleicht gesagt, ich bin eine unbescholtene Bürgerin, ich werde wahrscheinlich nie eine große Straftat begehen. Was wollen Sie mir anlasten? Was habe ich zu verbergen? Und je mehr Sicherheitstechnologien kommen, desto feindlicher bin ich dem ganzen gegenüber eingestellt. Ich benutze von zu Hause aus beispielsweise kein Internet mehr, ich gehe nur an öffentliche Internetgeräte. Klar man kann meine Daten wahrscheinlich trotzdem auf mich zurückverfolgen, zum Teil, aber ich bin da einfach doof, ich weiß überhaupt nicht, was da alles möglich ist und ich verwalte Daten auf meinem privaten Computer, die da besser im Netz nicht rumschwirren, also gehe ich nicht mehr von meinem privaten Gerät ins Netz.

Und vielleicht, wie sieht es in Ihrem Umfeld aus?

Privates Umfeld?

Egal, es wird ja dort so ein bisschen beschrieben, dass Peter z. B. die einen oder anderen Leute aus seinem Umfeld nicht verstehen kann. Sehen Sie das genauso, oder wie reagiert Ihr Umfeld? Ist es genauso sensibel wie Sie oder...?

Sehr unterschiedlich. Also ich kenne Leute, die durchaus ganz kritisch sich mit der Thematik befassen und auch sehr interessiert gewesen wären, hier heute dabei zu sein. Ich kenne Leute, die mich mit großen Augen angucken, was willst du denn da, was ist denn daran interessant? Ich denke es gibt auch genug Leute, die sich nicht damit befassen, die das so über sich ergehen lassen. Am Flughafen aufregen tun sie sich im Augenblick alle, wenn sie ihre Getränkeflaschen auskippen müssen.

Ich denke gegen die Technologien kann man sich nicht wirklich wehren, wenn man sich jetzt gegen alles stellt, dann darf man im Grunde gar nichts machen. Also mein Gedanke ist halt immer, was haben wir überhaupt für einen Einfluss drauf, auch wenn wir jetzt einen Fragebogen ausfüllen, das ist ja alles schön und gut, auch ist es interessant mal kennen zu lernen, was es für Technologien gibt, die ich vorher alle nicht kannte, aber was haben wir wirklich für einen Einfluss darauf. Plötzlich wird ja dann doch alles irgendwo eingeführt, mit Sicherheiten am Flughafen und sonst wenn wieder irgendwas vorgefallen ist, gibt es wieder neue Technologien und wir haben doch keinen Einfluss drauf. Also es ist so ein bisschen zwiespältig. Auf der einen Seite ist unsere Meinung gefragt und wir können sagen wir wollen das nicht, wir wollen nicht so überwacht werden, aber es wird auf der anderen Seite doch gemacht.

Es waren ja auch verschiedene Szenarien beschrieben, z.B. auch Szenarien z. B. zur Benutzung von öffentlichen Verkehrsmitteln, wo diese in den Szenarien die Möglichkeit einfach gab, sehr bequem etwas nutzen zu können, als auch mit etwas Aufwand das ganze anonym nutzen zu können. Also es beschränkt sich jetzt nicht nur auf Technologien, die sozusagen von der öffentlichen Verwaltung oder vom Staat eingeführt werden, sondern auch um Technologien, die von Privatorganisationen eingeführt werden und wo es einfach Wahlmöglichkeiten gibt.

Richtig ja.

Ja um manches zu vereinfachen, was weiß ich, um Zug zu fahren, dass man das mit Fingerabdruck oder sonst wie machen kann, das ist natürlich verlockend zu hören, wenn man

sieht, wie schwierig es manchmal ist, um eine Fahrkarte ran zu kommen. Aber auf der anderen Seite, wenn dann natürlich, wenn das meine Daten dann überall gespeichert werden, und jeder verfolgen kann, wo ich mit dem Zug hinfahre und das finde ich dann wiederum auch nicht gut.

Es wurden ja schlichte, relativ schlichte Alternativen aufgezeigt. Z. B. man kann entscheiden, will ich einen Vertrag mit irgendeinem Handyanbieter oder will ich eine Prepaid-Karte und schon hab ich mich ein Stück weit anonymisiert in dem ganzen.

Ja ja das stimmt.

Und das wäre ja auch möglich, dem gegenüber zu stellen. Der eine geht mit seinem Fingerabdruck in den Bus und der andere sagt aber ich habe eine Karte vorausgezahlt, es muss nicht jeder verfolgen wo ich hinfahre.

In Deutschland muss man aber derzeit noch Prepaid-Karten, also die Handys dazu, die Telefonnummern werden registriert, man muss einen Ausweis vorlegen. Ohne keinen Ausweis keine Freischaltung.

Meine Meinung widerspricht das dem Telemediengesetz. Da steht noch schärfer als im Teledienstedatenschutzgesetz vorher drin, dass pseudonyme und anonyme Nutzung ermöglicht werden muss, soweit es technisch möglich und zumutbar ist. Ich sehe da weder eine technische Unmöglichkeit noch eine Nichtzumutbarkeit.

Recht haben und Recht kriegen.

Ja. ...Müsste man sich mal irgendwie engagieren. Ich bin noch nicht dazu gekommen.

Also zu dem Thema sehr erschreckend fand ich das Vorratsdatenspeicherungsgesetz, d. h. die Telekommunikationsunternehmen werden verpflichtet, auf Jahre hinaus die Daten zu speichern, um sie im Nachhinein in ein paar Jahren auszuwerten. Das ist für mich persönlich ein sehr großer Eingriff in die Privatsphäre, hat nichts mit Verbrechensbekämpfung, ich möchte nicht Terrorismus sagen, zu tun. Das hat überhaupt nichts mit der buchungstechnischen Abrechnung von irgendwelchen Dingen zu tun. ... man kann sagen, zwei Jahre, drei Jahre, 10 Jahre und dann sollte das Thema erledigt sein, aber die echten Verbindungen zu speichern, das finde ich nun wirklich ein starkes Stück. Da können nur Dienste dran Interesse haben, die Dienste, wir sehen die Bundesrepublik, wir sehen vielleicht Europa, ich sehe die Dienste schon weit außerhalb von Europa.

Als erstes werden sich da die Firmen und Musikindustrie drauf stürzen, die gegen die bösen Filesharer vorgehen wollen. Ja, das haben wir auch schon des Öfteren gesehen, dass die erstmal sinnlose Anklagen erheben und ...

Ja für solche relativ banalen Geschichten werden solche Datenmengen verwaltet, nicht, und gespeichert und hier diese Idee in dem Fragebogen, dass Temposünder erfasst werden über Satellit. Also ich finde das fast skurril.

Aber kein Szenario, das was nicht umgesetzt werden kann.

Das war ja klar.

Wenn ich jetzt auf die Autobahn fahre, nach Hamburg, dann sehe ich nicht ein, eine Mautstelle nach der anderen und jedes Mal wenn man darunter fährt macht es Blitz und die Firma, die das betreibt weigert sich bis heute Auskunft darüber zu geben, welche Daten gespeichert werden und an wen sie verkauft werden. Das ist Privatunternehmen, das ist also keine staatliche Firma, sondern es ist ein Privatunternehmen, was Daten sammelt von jedem, der da durchfährt.

Es darf sie nicht sammeln, weil ...

Die geben aber keine Auskunft darüber.

Der Toll Collect-Vertrag ist immer noch nicht offengelegt, das finde ich sowieso schon ein Ding für sich.

Also es kann ja auch sein, dass sich das Finanzamt bestimmt freuen würde zu wissen, ob meine Dienstfahrten wirklich Dienstfahrten sind und für die Autoversicherung, keine Ahnung, ist das doch irgendwie interessant, ob derjenige ganz viel fährt, dann wird die Versicherung teuer.

Versuchen wir das Gespräch mal weiter zu lenken, dass jetzt vielleicht, aus der Gruppe hört man das ja schon, vielleicht so ein bisschen etwas provokative Frage und zwar die nächste wäre, wo Sie die positiven Eigenschaften und das Potential von der Sicherheitstechnologie sehen. Sie brauchen keine Angst haben, danach kommen auch noch die negativen Effekte. Dabei gibt es auch positive Effekte. Es gab ja, der Fokus lag jetzt so ein bisschen sehr auf Verbrechensverfolgung, aber in diesen Szenarien ist auch angeklungen, auch dieser Servicegedanke. Vielleicht dass man das auch noch mal in den Fokus mit einbezieht, natürlich wäre auch ein möglicher positiver Effekt natürlich

Das erste was mir da jetzt einfällt, das ist diese automatische Warnung, wenn sich, das Handy von der Carla jetzt irgendwie einen Tag lang nicht bewegt oder so und dass dann vermutet wird, dass irgendwas passiert ist. Das kann man auch andersrum regeln, das kann man auch so regeln, dass das Handy feststellt anhand von GPS-Daten. Ich hab mich jetzt einen Tag lang noch nicht bewegt, jetzt reg ich einen Notruf an, das da nicht irgend ne Stelle außen kontrolliert, ob das Handy bewegt wurde, sondern dass das Handy das eben selber feststellt.

...und dass diese geistig ja absolut gegenwärtige Frau selbst entscheidet, möchte ich diese Funktion haben oder möchte ich die nicht. Ebenso die Idee einen Chip in die neuen Autos einzupflanzen. Das Auto ist permanent ortenbar, will ich das oder will ich es nicht. Jetzt wird behauptet, dass das nur bei einem Unfall aktiviert wird, aber ich kann jederzeit geortet werden mit meinem Auto und ...

Es fing ja auch an mit dieser komischen Karte, die man da vorab bezahlt hat für was weiß ich U-Bahn oder so, die auch also in diesem Szenario war das drin, die auch irgendwie im Handy oder so integriert war.

Das waren zwei verschiedene Modelle. Das eine war die anonyme Karte, die nicht im Handy eingebaut ist, sondern fest aufbewahrt wird. Das andere war, dass man sich quasi mit seinem Handy am Bahnhof identifiziert, ich steig jetzt hier ein und steig woanders wieder aus, und wird automatisch abgerechnet.

Das hab ich nun nicht gelesen.

Das mag für einige bequem sein.

Nenn ich nicht Service ehrlich gesagt.

Die Mehrheit der Menschen merkt es ja gar nicht, sie lassen sich auch überall Chipkarten in Supermärkten andrehen und dann kriegen sie einen Bonus von 1% nach 100 Einkäufen und 100 Einkäufe lang wird registriert, der Kunde XY mit dem Altersprofil sowieso hat dieses eingekauft. Dann kann man gezielt Werbung schicken, die Adresse ist miterfasst. Diese Daten werden teuer gehandelt.

Es muss ja nicht immer ne Chipkarte sein.

Die meisten Leute nehmen das doch hin.

Ich verstehe, ich habe eine Payback-Karte.

Aber das ist ja letztlich keine Sicherheitstechnologie.

Nein aber es mit ein ... die Möglichkeit zu verknüpfen mit Datenbanken, das ist das Schlimme dabei.

Ihre Frage positive Sicherheitstechnologie, da möchte ich ein bisschen nicht in den persönlichen sondern in den geschäftlichen Bereich einfach mal eingreifen. Positiv, nehmen wir mal an, diese Verfolgung mit dem Auto, das können sie sich genauso vorstellen, diese Szenarien gibt es und das ist auch Realität. Die haben große Chipcontainer, die werden auch entsprechend getaggt, markiert, und die können über GPS verfolgt werden, wo befindet sich der Container, befindet er sich auf einem Schiff, wo, an welcher Stelle befindet er sich im Hamburger Hafen. Eine enorm hohe Sicherheit, man weiß genau wo er sich befindet, einmal zur Logistik und zum anderen, weiß ich auch, dass er noch da ist. Das ist ja ganz wichtig. Das geht aber nicht in den persönlichen Bereich rein, aber in den persönlichen Bereich, ja, ja, in den persönlichen Bereich, überlegen Sie mal die Sicherheit, Sie wollen ein Medikament kaufen und dieses Medikament ist mit Sicherheitstechnologie markiert worden, damit Sie ganz sicher sind, dass Sie auch das echte Medikament und keine plumpe Fälschung bekommen. Da halt ich das für die Gesundheit der Menschen, also muss ich sagen, für sehr wichtig, dass ich auch sicher bin, dass ich ein Medikament verabreicht bekomme, was ich auch oder was mir der Arzt verordnet hat. Ist aber kein Eingriff in die Persönlichkeitsrechte. Verstehen Sie, es wurde gefragt wo ist es sicher.

Ja das ist aber, ja diese Technologie, die da angesprochen wird, die ist ja mal aus diesem Grund entwickelt worden, die ist ja mal von FedEx entwickelt worden, um die Pakete zu verfolgen und auch um feststellen zu können, an welcher Stelle ein Paket einfach irgendwie verloren geht und auch mit Containern kann ich das noch einsehen, aber Medikamente, man kann diesen Text einfach klonen, das ist ganz einfach die auszulesen und die zu kopieren ist sogar einfach, d. h. wenn jemand Medikamente fälscht, für den wird das ...

Erstmal ist das ja was Positives, es geht ja erstmal und das Positive. Dass man was fälschen kann, dass ist überall möglich, denk ich mal. Aber das Positive ist erstmal, das so was möglich ist. Es ist auch positiv, dass man eben mit der Bahn fahren kann mit weiß was ich mit einer Chipkarte oder mit einem Handy, ohne dass man sich umständlich ne Fahrkarte kaufen muss.

Aber sobald dieser Text bei Medikamenten kostengünstig gefälscht werden kann, und das können sie, sobald sich mal einer die Mühe gemacht hat, eins davon genauer auseinanderzunehmen, sind sie wertlos.

Ja das ist das Negative, wir sind ja gerade beim Positiven. Also ich hab das mit dem Bahnfahren, das muss ich auch mal eben noch mal sagen, meine Mutter hatte neulich, die konnte bei der Bahn nicht mitfahren, sie durfte nicht mitfahren, weil der Fahrkartenschalter nicht funktionierte und sie kam an keine Fahrkarte ran, denn im Zug wird keine mehr verkauft. Also ich mein irgendwo natürlich, braucht man da mehr Personal.

Da würde ich trotzdem einsteigen, die wissen genau welche Automaten nicht funktionieren, das ist nachvollziehbar.

Es geht ja um das Positive.

Das ist aber nicht positiv, das ist jetzt irgendwie vergleichbar, als wenn wir uns darüber unterhalten, das wir mit dem neuen Auto auch 250 fahren kann, während die Bremsen aber nur für ein Auto ausgelegt sind, was 100 fahren kann. Dann ist es nicht positiv, dass wir schneller fahren können.

Dass es so eine Wahlmöglichkeit gibt an sich finde ich positiv. Ob ich das jetzt wirklich nutzen würde, weiß ich nicht.

Doch die Leute dies machen wollen, können es gerne.

Ja.

Ich weiß nicht, ob ich es machen würde.

Ich weiß es selbst auch nicht, aber ich finde es grundsätzlich erstmal positiv. Auch das mit den Medikamenten. Erst mal finde ich es positiv, aber es gibt immer Möglichkeiten, das zu fälschen.

Es wird gefälscht werden und deswegen sollte man es gar nicht erst machen.

Dann könnte man jetzt auch z. B. anführen, diese Idee, die es mal gab mit der Krankenkasskarte, dass z. B. Diagnosen, die gestellt worden sind, gespeichert werden und dass denn der nächste Arzt weiß, da liegt eine Allergie vor, z. B., das ist ja ganz toll. Aber mal ganz ehrlich, ich hab nun gerade ne ganze Menge Allergien, die aber nicht erkannt worden sind, also ich bin bei mehreren Ärzten gewesen, die nicht in der Lage waren das zu erkennen und das sind so Sachen, da hätte ich jetzt die ganzen Fehldiagnosen auf dieser Karte stehen, was wiederum letztendlich gesehen bei dem, der es erkannt hat, die ihn wahrscheinlich nur ... hätte. Also es ist nicht unbedingt immer alles positiv, auch wenn es sich im ersten Moment so anhört.

Sie wollen mehr oder weniger schon fast aufs Negative hinaus. Negativ würde ich sehen, wenn ihre Krankenkasse weiß, aha, es ist entdeckt worden, dass eine Allergie vorliegt und jetzt müssen sie sofort die Krankenkassenbeiträge erhöhen. Die Verknüpfung der Daten, das halte ich persönlich für eine Gefahr. Das ist das Entscheidende.

Deshalb sollten diese Datensätze auf der Gesundheitskarte ja auch verschlüsselt werden, sodass man sie mit einer Arztkarte auslesen kann. Auch das wird von kriminellen Elementen irgendwie umgangen werden, dass sie trotzdem rankommen.

Ein ganz schlichtes Beispiel, wo solche Technologie eben ein gutes Gefühl macht, z. B. Kameras. Es gibt Plätze, dunkle Plätze, wo ich sag, das ist ganz schön eine Kamera zu sehen, ob sie an ist weiß ich nicht, aber an manchen Stellen kann es mir durchaus ein Gefühl der Sicherheit geben.

Aber an manchen Plätzen würde es vielleicht reichen, wenn die ordentlich beleuchtet sind.

Das wäre natürlich noch schöner oder es wäre Personal da. Klar. Es gibt immer ne bessere Lösung.

Es hat da auch schon Experimente gegeben, dass Ecken, die vorher videoüberwacht wurden, dass da einfach eine Lampe hingestellt wurde und schon war es da aus mit der Kriminalität, weil man sieht ja bei den Kameras nicht, ob da gerade aktuell jemand auf diesen Monitor guckt und selbst wenn, das ist so eine Batterie von Monitoren, da kann die arme Person dahinter gar nicht rechtzeitig gucken, was da los ist und selbst, wenn sie was sieht, wie lange dauert es, bis die Polizei dann da ist.

Das sind einmal das passive und einmal das aktive Videosystem. Das aktive erkennt sofort verdächtige Bewegungen und Personen.

Auch da hab ich irgendwie Schwierigkeiten, weil derjenige...

Das hilft auch nicht, selbst wenn das sofort erkannt wird. Wenn ich jemand auf seinen Kopf hau und das Portemonnaie klaue und weglaufe, dass man mich nicht erkennen kann, so schnell ist die Polizei nicht da, dass man mich erwischt.

Das hat sich ja nun bei aktiven Kameras auch herausgestellt, dass die Leute, die das beobachten, die die Kameras steuern, eigentlich mehr den Mädels hinterher gucken, die mit den kurzen Röcken, und dass die gleichen Sachen nicht beobachtet werden, also das ist auch so

Vielleicht der Frau Merkel ins Wohnzimmer gucken.

Vielleicht kann man das gleich noch mal nehmen, um den nächsten Punkt anzusprechen. Und zwar über welche negativen Entwicklungen man von Sicherheitstechnologie eigentlich verärgert ist. Ist das eigentlich die, dass sie da nicht dafür genutzt werden, wo wofür sie eigentlich gedacht sind, oder dass man danach guckt, das Positive, das Negative und auch da vielleicht einfach mal guckt. Vielfach wurde ja angesprochen, ich weiß eigentlich nicht wofür ich mich entscheide. Kann man das noch weiter definieren, um oder was würde einem helfen, das Positive vom Negativen zu trennen z. B...

Also erstmal muss ich sagen, dass ich mich generell, wenn ich irgendwo so eine Kamera am dunklen Ort sehe, dass ich froh bin, dass sie da ist. Auf irgendwelchen U-Bahnstationen, wenn ich da ganz alleine bin und da kommt irgendwie so eine Horde wilder Leute an, kann ich wenigstens hoffen, dass man die hinterher noch erkennen kann oder so, und ich hoffe natürlich, dass die Leute nicht so gut informiert sind und auch nicht wissen, dass da gerade keiner hinter sitzt.

Das geht mir völlig genauso. Sonst ist die Wirkung dahin.

Ja, man geht immer davon aus, da ist denn auch wirklich jemand da. Und wie gesagt, wenn da jetzt wirklich so eine Horde kommen würde, wo ich denn vielleicht noch vorbeigehen soll, dann bin ich auch froh, wenn da ne Kamera ist und denke vielleicht haben die die auch gesehen. Weil die abschreckende Wirkung, so glaube ich, hoffe ich, dass sie da ist. Hoffe ich.

Tja. Nur werden die Kameras immer kleiner. An manchen Stellen, wo Kameras hängen, sollte man auch drauf achten, dass es schöne deutliche und sichtbare Kameras sind.

So wie diese Dinger, die blitzen beim Verkehr, wo man genau weiß, da muss man jetzt langsam fahren und danach kann man wieder Gas geben.

Die können von mir aus gerne überhaupt nicht zu sehen sein.

Zur Kameradiskussion würde ich ganz gerne noch die Frage stellen. Gestern stand meines Erachtens in den Kieler Nachrichten, dass die KVG sich nicht oder die Stadt selber der Rat sich nicht dazu durchgerungen, in den Bussen der KVG Videokameras zu installieren, was in vielen Städten, bundes-/europaweit, schon Gang und Gebe in S- und U-Bahnen ist und in vielen Städten auch in den Bussen. Sie haben sich nicht dafür entschieden, aus Kostengründen, so nach dem Motto, die Installation kostet mehr als der Vandalismus, der auftritt. Für uns ist es ja wichtig, wie fühlen wir uns persönlich in unseren eigenen Bürgerrechten eingeschränkt. Eben hat es in der Diskussion angeklungen, es ist ein subjektiv besseres Gefühl, wenn man weiß, dass da an bestimmten kritischen Orten eine Kamera ist.

Also gerade in Bussen ist ja immer noch der Busfahrer und ja o. K. wenn da jetzt die 82 fährt und vollgestopft ist mit Studenten, da kriegt man das dann schon mal nicht mit, wenn da ganz hinten irgendwas los ist, aber im Allgemeinen sollte das doch wohl möglich sein, dass man was mitkriegt, wenn da irgend einem Menschen etwas angetan wird und ansonsten völlig richtig, die Installation der Kameras kostet mehr als der gesamte Vandalismus kostet. Insofern ist es gegen Vandalismus nicht sinnvoll. Gegen Gewaltverbrechen hilft es auch nichts, selbst wenn man die Leute hinterher identifizieren kann, wird davon nicht relevant viel verändert.

Ich denke schon, wenn man wüsste, dass es beispielsweise nur eine kurze Zeit lang gespeichert wird und dann auch wirklich gelöscht wird, dann könnte ich mich damit anfreunden. Nun fahr ich keinen Bus, von daher ist es ein schlechtes Beispiel, aber das wäre halt so eine Sache, dass, wenn sie eben klar- und offenlegen, dass das denn wirklich nur für sag ich mal 2 Tage und feststeht, hier auf dem U-Bahnhof ist nichts passiert, dann wird der ganze Scheiß auch wieder gelöscht, dann würde ich das auch nachempfinden.

Wir haben jetzt ja über negative Sachen und positive Sachen diskutiert. Vielleicht dass man das jetzt noch mal auf en Punkt bringt, oder die Fragestellung diskutiert, wann ist die Sicherheitstechnologie wichtiger als die Privatsphäre und umgekehrt. Kann man das voneinander abgrenzen?

Also früher hätte ich immer gesagt, auf jeden Fall, und in punkto Terrorismus und Kinderpornographie, das ist ja auch immer so ein schönes Schlagwort, da gibt es keine Gnade. Aber nach dem, was jetzt hier mit dem G8-Gipfel passiert ist, wo einfach willkürlich Leute da ganze Wohnanlagen durchsucht worden sind, nur aufgrund der Tatsache, weil sie ne andere Meinung haben, frage ich mich schon inwieweit da Möglichkeiten bestehen das auszulegen,

wie einem das passt. Ich halte also auch, muss ich jetzt leider sagen, jemand der ein Polizist ist, ist auch nur ein Mensch und ich bin z. B. mit einer zur Schule gegangen, die kann ich auf den Tod nicht ausstehen, die ist zur Polizei gegangen, für mich keine Person meines Vertrauens und von daher weiß ich nicht, ob man den Leuten nicht auch ein bisschen zu viel Macht in die Hand gibt, da einfach was zu konstruieren um sich das hin- zurechtzubiegen um denn da Sachen durchzuführen, die gegen sämtliche Grundrechte verstoßen und dass die Leute nicht mal irgendwelche Konsequenzen davontragen müssen, das ist das, was mich an dieser G8-Geschichte so wütend macht. Der Gipfel selber hat mich gar nicht so interessiert.

Wir können uns nicht darauf verlassen, dass diese Datenauswertung immer korrekt ist und dass dabei alle legalen Bedingungen erfüllt werden.

Ich gebe ein anderes Beispiel. Wenn jetzt z. B. bei uns irgendjemand umgebracht wird und man findet da irgendwelche genetischen Spuren, dann werden ja sämtliche Männer aufgefordert, Speicheltest abzugeben und das wird aber nicht wieder gelöscht, das heißt also es gibt hier Dörfer oder Orte, in denen hier mehrere tausend Menschen ihre Daten oder ihren Speichel abgegeben haben, die stehen für den Rest aller Tage in der Straftäterdatei.

Das hab ich also von den Leuten in der Uni-Klinik, die mit so was vertraut sind, allerdings anders gehört. Die haben da zwei separate Tabellen, einmal eine Tabelle mit den Gen-Daten und dann die Tabelle mit der Zuordnung der Gen-Daten zu Personen, und diese Tabelle wird dann nach 2, 3 Jahren oder nach Abschluss der Ermittlungen dann wirklich gelöscht. Die Daten, die sie dann über haben, die sind dann nicht mehr zu den Personen zuzuordnen, die brauchen die aber für die Statistiken, um auswerten zu können, was für Unterschiede wirklich geeignet sind, um festzustellen, ob irgendwas wirklich unterschiedlich oder gleich ist.

Noch mal zur Fragestellung. Wann ist Sicherheit wichtiger als Privatsphäre und umgekehrt? Wir haben hier zwar so einzelne Sachen diskutiert...

Ich will das jetzt mal weiter mit diesen verknüpften Datenbanken, jetzt beispielsweise, zum Beispiel mein Vater in so einem Einzugsgebiet wohnt und der jetzt irgendwie so eine Probe abgeben musste, der steht für den Rest aller Tage in der Sexualstraftäterdatei. .. interessiert es doch keinen mehr, wie er da rein gekommen ist. Dass er zum Beispiel freiwillig da hingegangen ist oder so. So etwas gebe ich jetzt mal als Beispiel zu bedenken, sondern der steht da einfach drin und das wird jetzt beispielsweise die nächsten Arbeitgeber garantiert interessieren.

Das heißt also, das ist eher so, dass die Privatsphäre überwiegt.

Aber es ist freiwillig abgegeben worden. Nur diese Leute sind dann halt nicht informiert.

Genau in dem Fall haben ja Leute geklagt, die gesagt haben, sie würden es abgeben, wenn es denn danach gelöscht wird und da haben die damals ermittelnden Behörden sich schlichtweg geweigert. Nein, machen die nicht und das ist denn auf so ein Dorfmobbing hinausgelaufen, weil die denn alle so och die wollen das nicht.

Dass diese Stellen sich wider geltendes Recht weigern, diese Daten zu löschen, das kann nicht angehen.

Ja weil dass der Staat sich nicht mal an Grundrechte hält, haben wir ja nun vor ein paar Wochen und Tagen gerade erst gesehen.

Ich erinnere mich an diesen, ich hab den Namen vergessen, ein kleiner Junge entführt und man fürchtete, dass Kind ist tot und dann find ich zum Beispiel, wenn dann jemand unter unmittelbarem Tatverdacht steht mit richterlichem Beschluss zu sagen jetzt wird in eine Wohnung eingedrungen, das ist ja auch Verletzung der Privatsphäre. Sei es jetzt durch Abhören oder durch Eindringen, das kann ich vielleicht noch nachvollziehen und akzeptieren. Aber es muss der richterliche Beschluss her. Dann ist das ganze kontrolliert und unkontrolliert darf das meines Erachtens nicht passieren.

Und ohne gravierender Straftat, das kann also nicht sein hier wegen Steuerhinterziehung oder...

...wegen Temposünden und nicht wegen was war das noch für ein lächerliches Beispiel, Versicherungsgeschichten.

Ja.

und auch nicht ob ein Auto geklaut ist oder nicht.

Was das jetzt zum Beispiel in dem Zusammenhang ergeben hatte, haben jetzt Leute bei denen an der Tür geklingelt und behauptet sie würden vom Sozialamt kommen und würden ne Routinekontrolle machen und auf Nachfrage im Nachhinein hat dann ergeben, dass das Sozialamt gar keine geschickt hatte und solche Spielchen, das sind so Sachen, das kann nicht sein. Weiß ich nicht. Das sind eigentlich die Methoden, wie man sie von GEZ her kennt.

Das heißt, irgendwann kippt es dann und also pro Privatsphäre ab einem bestimmten sag ich mal Level der Bedrohung oder der Straftat und man möchte gerne noch sozusagen ne zweite Autorität mit dabei haben.

Mindestens.

Ja mindestens.

Es sollte drauf geachtet werden, dass das alles mehrfach kontrolliert wird, dass man nicht alleine die Polizei, die Ermittlungsbehörde, entscheidet, wo sie nun abhört und belauscht, sondern dass da eben auch, das da eben ein Richtervorbehalt ist. Und sowieso sollte es nur erlaubt sein, bei ausreichend schweren Straftaten, zum Beispiel sollte nicht der Internetverkehr abgehört werden dürfen, bloß weil da irgend so ein Unternehmen meint, der tauscht meine Filme aus, ohne mir was zu bezahlen.

Wenn man das ganze weiterspinnt mit Datenverletzung, was liefern wir für Daten und wirklich noch freiwillig. DNA-Daten werden irgendwann abgeglichen mit meinen persönlichen Gesundheitsdaten und irgendwann haben wir die schöne neue Welt und irgendein Big Boss entscheidet, ob ich mich noch vermehren darf oder nicht. Wir sind ja in dem wildesten Sciencefiction drin.

Das ist ja im Grunde der Punkt. Ihre Daten, die Daten Ihres Mannes, der Eltern...

Ist das noch kompatibel, kommt dabei was raus oder nicht?

...der Geschwister. Also versichern wir das Kind gleich zu ganz anderen Bedingungen. Das kommt dabei raus. Diese Informationsverknüpfung, die halt ich nicht für in Ordnung, da wird absolut in die Privatsphäre eingedrungen. Und was noch viel schlimmer ist, wenn Sie sich die größeren Unternehmen heutzutage angucken, die ja alle unternehmensmäßig verflochten sind, das fängt bei der Bank an, das geht über die Versicherung und über größere Kaufhäuser. Jetzt haben Sie die totale Verknüpfung. Das heißt die Banken können die Informationen an die Versicherungen geben, ja und umgekehrt, aha, wir wissen, da ist ein Defekt, Gen-Defekt oder irgendwas, also gibt's den Kredit nicht in der Höhe. Die Firmen haben die Möglichkeit, dann Risikoeinschätzung ganz anders durchzuführen, obwohl es gar nicht an dem ist.

Ein schönes Beispiel. Ich hab mich mit einem Freund ausgetauscht, der längere Zeit Hartz IV-Empfänger war und ich verdiene relativ gut und wir kamen irgendwie drauf, ich krieg immer Werbung von Banken, wo ich mein Geld schön anlegen kann. Er kriegt immer Werbung von Banken für Kredit. Ach das ist ja interessant, nun veränderte sich meine Einkommenssituation, weil ich auf halbe Stelle gegangen bin und die nächste Post von einer Bank war ein Kreditangebot. Da hab ich auch gedacht, dass das bestimmt kein Zufall ist.

.. Stellen Informationen schon verkauft.

Meine Bankdaten scheinen irgendwo ganz schnell die Kurve gemacht zu haben.

Also die Bank kennt Ihr Einkommen, entsprechend

Das war nicht meine Bank, die mich beworben hat.

Sie wissen ja gar nicht, wie die Banken untereinander verknüpft sind.

O.K. wir haben jetzt über einzelne Auswirkungen gesprochen.

Was ja zu akzeptieren ist.

Die meisten Banken stehen alle im selben Rechenzentrum.

Ich habe noch einen Satz mir notiert aus dem Fragebogen. Und der interessiert mich sehr. Wir liefern ja auch über viel mehr noch nicht nur über meine Bankgeschäfte, sondern über mich als Mensch meine Fingerabdrücke, meine Iris, womöglich meine DNA, kursiert sonst wo und jetzt steht da dieser schöne Satz: Ist Einsatz von biometrischen Daten einmal geknackt, so ist er für immer verloren. Gibt's mich dann nicht mehr. Ich weiß nicht, was bedeutet das? Das find ich also so schockierend, was ich womit ich mich ausliefere an eine Überwachung.

Vielleicht ist das auch ne schöne Überleitung zu dem nächsten Punkt. Wo es einfach, wir können das ja später nachher gerne noch mal diskutieren, wo es darum geht, welche Gruppen sollten mit einbezogen werden, wenn darüber entschieden wird, dass oder wie neue Sicherheitstechnologie eingeführt werden. Wer sollte an dem Entscheidungsprozess beteiligt werden?

Also am Wenigsten die Politiker.

Ja, ganz genau.

Am Wenigsten...

Keine wirtschaftlich interessierten Institutionen.

Also letzten Endes ist das merken wir hier ja schon an der Diskussion, ist das ein fachlich so hochspezifisches Thema, wenn ich hier in die Runde fragen würde, was irgendwelche Securitydinge bedeuten, dann würden auch sicherlich alle Kopf schütteln, nichts mehr verstehen und genauso ist es in dieser Sicherheitsdiskussion. Die wenigsten verstehen überhaupt worüber sie diskutieren. Deshalb ist es sehr schwierig, auch sicherlich für Sie als Datenschutzmann, diese Informationen überhaupt klar zu machen geschweige denn eine Diskussion beziehungsweise eine Findung eines Kompromisses oder dergleichen. Politiker, die verstehen das Thema ohne nicht.

Und wir sind nicht unbedingt der Querschnitt der Bevölkerung, der hier sitzt, glaube ich.

Der Querschnitt der Bevölkerung sagt, was interessiert es mich, der tritt den Brief in die Tonne und kommt nicht und ja hier sitzen eigentlich nur Leute, die irgendwie daran interessiert sind.

OK. Dann mal die provokative Frage, an so einem Entscheidungsprozess, egal ob man jetzt dafür oder dagegen ist, Fachmann oder nicht, sollten trotzdem alle oder viele Gruppen beteiligt werden oder dass man sozusagen wie das so ein bisschen durchklingt eher auf die psychische. Es ist ja auch so, wenn mehrere Gruppen daran beteiligt sind, man reibt sich ja auch aneinander.

Also die Wirtschaftsunternehmen, die diese Technologien produzieren und eingesetzt haben wollen. Philipps z. B., will sein RFID-Text natürlich möglichst überall eingesetzt haben. Da verdienen die nämlich Geld dran. Die dürfen gerne ihre Meinung dazu sagen, aber auf keinen Fall sollte nur auf die gehört werden.

Und dann denke ich bei der Beteiligung von, wer wird beteiligt ist erstmal entscheidend, es muss an Aufklärung her. Was eigentlich alles passiert, was an Missbrauch möglich ist. Solange da kein Mensch drüber Bescheid weiß...

Es hat sich gerade jetzt vor ein paar Tagen erst gezeigt, dass es Gutachten gab, ich glaub so ein Stapel an Papier, die bewiesen hat, dass beispielsweise der Reisepass und gewisse Gesetzesvorschläge einfach überhaupt gar nichts ... sind Berufsverbände da hingegangen, es sind Juristen da hingegangen, die sind gehört worden und trotzdem wurde genau das beschlossen, wo alle gesagt haben, das taugt überhaupt gar nichts. Also was die Politiker angeht, tut mir leid, in meinen Augen verfolgen die nur ihre eigenen Zwecke, da müssen Fachmänner ran, zumindest für die Entscheidung darüber, ob so was gut ist oder nicht. Da müssen Fachleute hin.

Wenn es um politische Entscheidungen geht, dann kann man die Politiker ja nun nicht ganz ausschließen.

Politiker sind wirklich echt ...

Als gewisse Sicherheitshysteriker gehören längst Es gab in der angesprochenen Entscheidung gab es auch einen Politiker, OK die Linken waren auch mit dabei, die waren auch dagegen, die sich durchaus informiert haben und drauf gehört haben, was ihnen gesagt wurde und die dann auch dagegen waren. Aber der ganze Rest hat gesagt, meine Fraktion will das so, ich will nachher wieder mit drauf auf die Landesliste. Also muss ich wohl so entscheiden, wie die Fraktion das will.

Dazu muss ich mal sagen, das hat auch weiterführende Konsequenzen. Ich kann meine Partei nicht mehr wählen. Ich möchte aber auch eigentlich auch die nicht wählen, die ...

Wer trifft eigentlich die Entscheidung. Man kann die Politiker doch nicht ganz ausschließen. Es ist doch letztlich der Gesetzgeber, der die Entscheidung trifft, oder?

Die Frage war ja nach der Anhörung. Wer soll angehört werden.

Einbezogen, das ist ja generell ein sehr großer Begriff. Das spielt natürlich so was auch mit rein.

Also in der Schweiz klappt so was wesentlich besser.

.. überhaupt eingesetzt werden und wie das rechtlich dann auch machbar ist. Man kann den Gesetzgeber nicht ausschließen, da muss man natürlich Datenschützer mit einbeziehen, da muss man natürlich die Leute mit einbeziehen, die diese Technologien entwickeln, sonst, ich weiß nicht wer das sonst machen soll.

Wollen wir diesen Part mal ganz kurz mit aufgreifen, nur dass wir jetzt einfach vielleicht zwei Fragen oder Themenbereich mal zusammenbringen, denn der nächste Themenbereich wäre, was man bei der Regulierung oder bei dem Aufbau zur Einführung neuer Technologien beachten sollte. Das klang ja da schon so ein bisschen an, Politiker kann man nicht ganz ausschließen, aber vielleicht welche Anregungen oder Gebilde, welche man dort bauen kann, zu einer Entscheidungsfindung.

Also die Firmen beispielsweise halte ich ehrlich gesagt nicht für kompetent, weil die wollen ihren Kram verkaufen und das gibt also, die schaffen sich künstliche , um ihren Kram zu verkaufen, also gerade jetzt war wieder ein sehr gutes Beispiel, dass erwiesen worden ist, dass sie nichts taugen, dass sie innerhalb von 60 Sekunden zu knacken sind, aber eine Maschine, die die im Niveau vom PC von vor 10-15 Jahren entspricht, wird für 4.500 Euro verhökert, da sind natürlich Maden drin, das ist natürlich klar, dass die hinterher sind, dass das verkauft wird und da dürfen die halt überhaupt gar nicht also gehört werden schon, klar, aber nicht einbezogen werden in die Entscheidung. Ich hab den Eindruck, dass die wirtschaftliche Macht, die dahinter steht, einfach wesentlich größer ist als der Verstand.

Aber wer bleibt denn da noch übrig?

Unabhängige Ausschüsse. Also ich denke...

Das Unabhängige Landeszentrum für Datenschutz ...

Also das sind keine Politiker, das sind keine Leute aus der Wirtschaft und das sind, wer bleibt dann noch über,

Unabhängige Juristen, unabhängige Experten, unabhängige technische Experten.

Wobei unabhängig für mich in meinen Augen auch schon anfängt mit, der darf nicht in irgendeinem Aufsichtsrat oder sonst wo ...

Da haben die Deutschen sowieso ein Problem.

Wir sagen wir bezahlen unsere Politiker hoch, damit sie unabhängig und

Und das ist sowieso gleich der nächste Punkt. Ein Politiker, Politiker zu sein, Bundestagsabgeordneter zu sein, ist ein Vollzeitjob. Der hat keine Zeit in irgendeinem Aufsichtsrat zu sitzen. Der kann nicht im Aufsichtsrat sitzen.

Was sind denn unabhängige Menschen? Gibt es wirklich Menschen, die so unabhängig sind, dass sie überhaupt keinen Einfluss auf irgendwas üben?

Das weiß ich nicht, aber ein Bundestagsabgeordneter, der in irgendeinem Aufsichtsrat sitzt, den kann ich nicht mehr unabhängig genug nennen.

Ja, da geht es schon los. Gibt es wirklich unabhängige Menschen, ich glaub nämlich nicht dran, dass es unabhängige Menschen gibt, die da irgendwo Einfluss, jeder arbeitet in irgendeiner Firma oder in der Regierung oder in einer Behörde und, das geht doch gar nicht.

Ja in gewisser Weise ist es eine Frage der Wertschätzung. Ist es uns etwas wert, so viel wie möglich Unabhängigkeit herzustellen. Machen wir z. B. Geld locker, um eine unabhängige Kommission zu finanzieren, die nicht von anderswo gespeist wird, dann haben wir mehr Unabhängigkeit, als wenn ein ehrenamtliches Team einsetzen, das von Siemens oder Philipps gesponsert wurde.

Ja aber ich frag mich eben, die Unabhängigkeit find ich ja auch gut, ich glaub aber nicht dran, dass es wirklich so unabhängige Menschen gibt, die überhaupt keinen Einfluss ...

Aber man kann Unabhängigkeit begünstigen, oder eben nicht. Und begünstigt wird es ja offenbar nicht.

Ich würde echt lieber den CCC, den Foebud, den Förderverein für eine FFII, wie auch immer das ausgeschrieben heißt, die würde ich erheblich lieber in so einer Kommission sehen als Philips.

Kenn ich auch nicht.

FFII kenn ich auch nicht.

Förderverein, kann ich später nachgucken, aber FFII.org, auch so ein Haufen, der auf Datenschutz geht.

Sollte aus dieser Befürchtung, dass es niemanden gibt, der unabhängig ist, können daraus irgendwelche Regelungen oder Anforderungen erwachsen, die bei z. B. diesen Einführung von neuen Technologien beachtet werden sollten oder zwingend sind.

Ich denke z. B., dann man ne Unabhängigkeit erreichen würde, indem man ganz einfach den Leuten Nebenjobs verbietet, und ich denke das wird zur nächsten Legislaturperiode völlig andere Leute da sitzen, weil das für die

Also das wäre z. B. eine Form, dass man sagt, wer sich für ein politisches Amt dann bewirbt, das ausschließlich macht.

Und wenn der ne eigene Firma hat, dann muss er sich einen Stellvertreter suchen.

Gibt's da vielleicht noch weitere.

Derjenige, der etwas davon hat, dass eine bestimmte Technologie eingeführt wird, darf nicht dafür stimmen dürfen, dass diese Technologie eingeführt wird.

Aber dagegen?

Dagegen gern, ja.

Ja, aber z. B., dass jetzt, was weiß ich, irgendwas wirtschaftliches entschieden wird, dass beispielsweise, wenn denn irgendwie diese Partei von Siemens wurde jetzt genannt, gesponsert wird, dass man das einfach mal hinterfragt. Finde ich.

Es gibt da größere Lobbyorganisationen, die hintenrum von Firmen gesponsert werden und das weiß keiner, das interessiert auch keinen, aber natürlich versuchen diese Lobbyorganisationen dann dafür zu sorgen, dass Dinge passieren, die dieser Firma nutzen.

Und alles was nicht aufgelegt werden kann ist Bestechung und muss bestraft werden, tut mir leid. Wenn ich beim Finanzamt irgendeine...

Ich meine, es sollte auf jeden Fall beachtet werden, dass wenn es wirklich so weit sein sollte, dass im Vorwege auch die Information heraus gegeben werden, was gespeichert wird, wo gespeichert wird, wozu das gespeichert wird. Man sollte auch ganz klar und deutlich sagen, welche Informationen an den Verfassungsschutz gehen und sonstige internationale Organisationen. Ich mach jetzt mal ne Lücke auf und an privatwirtschaftliche Unternehmen, die evtl. Interesse an solchen Informationen haben. Das sollte auf jeden Fall bei der Einführung solcher Verfahren klar und deutlich gesagt werden.

Also mehr Transparenz.

In jedem Fall mehr Transparenz, so wie es an und für sich in der EU auch vom Gedanken her gefordert wird.

Ist ja alles vorgesehen, nur da wird sich dann auch gegen gesträubt.

Ja wir sehen es ja jetzt idealtypisch. Wie könnte das aussehen? Und so könnte und müsste das ganze aussehen, anders geht's nicht, sonst wenn ich 1. keine Ahnung von der Technologie habe, wenn ich 2. nicht weiß was geschieht da wirklich mit, ja, da kommt logischerweise Misstrauen auf. Und das ist das entscheidende. Und wenn ich ne Videokamera sehe und ich weiß nicht, was mit meinen Daten anschließend geschieht, kommt Misstrauen auf. Ich weiß nicht, wie lange es gespeichert wird, ich weiß nicht, welche Informationen überhaupt

gesammelt werden, logischerweise, das geht genauso bei den Fahrkarten, ist alles das gleiche. Sonst überall steht drauf für Risiken und Nebenwirkungen fragen sie ihren Arzt oder Apotheker, da sollte genauso draufstehen, wenn sie Fragen haben, rufen sie die und die an und wir informieren sie weiter oder rufen sie die und die Seite auf, da stehen sämtliche Informationen oder sie haben da eben schon so ein schönen Fleck drauf, den sie dann abfotografieren und dann wissen die sofort um was es da im Einzelfall geht.

Ich finde auch sämtliche Formen der Datenspeicherung muss dem Staat vorbehalten sein. Wenn z. B. Mordgeschichten oder so, das kann einfach nicht sein, dass das an Firmen abgetreten wird, wo nicht mal so ganz klar ist, wer daran jetzt irgendwelche Beteiligung hat. Also jetzt nur mal als Beispiel: ... ist ne Tochter von Mercedes Benz und Mercedes Benz gehört zu 25% dem Irak oder Iran, jetzt muss ich lügen.

Saudi Arabien.

Oder?

Ne Iran oder Irak. Ich muss jetzt lügen. Und eine von beiden...

Es war ja auf dem Fragebogen auch noch so schön die Menschenrechtsorganisationen verzeichnet, hier geht es um Menschenrechte. Warum sollen die nicht beteiligt sein? Und ich sehe schon Briefe aus anderen Ländern im Namen von ankommen.

Wir kommen auch langsam jetzt zum Ende. Die erste wäre, ob sich die Einstellung nach der heutigen Veranstaltung zu Sicherheitstechnologie geändert hat.

Nein. Die G8-Geschichte hat tüchtig reingehauen. Allein die Tatsache, dass man keine andere Meinung haben darf, finde ich echt ein Hammer. Ich glaube, wenn man die hätte demonstrieren lassen, dass dann überhaupt nichts passiert wäre und niemand darüber nachgedacht hätte. Aber das da so auf die Leute losgegangen wurde, das nachweisbar Polizisten oder irgendwelche Informanten in die Menge eingeschleust worden sind, die die Leute aufgepuscht und aufgeheizt haben, um dann da etwas zu provozieren. Das ist der Staat, in dem wir leben? Vor vier Wochen habe ich mich noch über die Amerikaner totgelacht, so nach dem Motto „die haben nicht einmal mehr die Demokratie“ Und irgendwie sind wir jetzt an dem gleichen Punkt. Und ich frage mich wirklich, wie mir das entgehen konnte.

Ich fragte vorhin Frau Raguse, und es war irgendwann in den letzten Wochen das Schlagwort in der Presse, dass bei Terrorverdacht nicht mehr die Unschuldsvermutung gilt.

Ja, sie haben jetzt so entschärft gesagt, dass das als Schlagwort in die Medien gekommen ist, das ist aber keine beschlossene Sache. Und da habe ich dann gedacht, wenn es soweit kommt, dann verabschieden wir uns vom Rechtsstaat.

Ja, genau.

Und was geschieht dann mit unseren Daten?

Frau Bundeskanzlerin Merkel hat auch gesagt, dass die Videoüberwachung von öffentlichen Plätzen so etwas ist, worüber man nicht reden darf, man muss es einfach machen. Nicht ganz genau mit den Worten, aber ziemlich genau.

Als ich in der Schule war und wir das Dritte Reich durchgenommen haben, da habe ich dann meine Oma gefragt, wie alt sie war und was sie damals gemacht hat. Und ich habe das einfach überhaupt nicht verstanden, dass sie sagte, dass das ganz normal war und irgendwie an ihnen vorbeigegangen ist. Und dass es zu spät war, als sie es bemerkt haben. Da habe ich immer gedacht, wie naiv man denn sein muss, um so was nicht mitzubekommen. Und irgendwie habe ich das Gefühl, dass wir irgendwie an den gleichen Punkt gehen, und wenn wir weiterhin aktiv bleiben, oder uns zumindest irgendwie engagieren, um den Rest an Demokratie zu bewahren, dann...

An der Stelle hätte ich da noch mal eine Frage. Zum Beispiel an den Datenschutz sogar. Kann ich mich dagegen wehren, dass ich Fingerabdrücke abgeben muss für meinen Reisepass? Ja? An welcher Stelle? Oder ist dann die Alternative, dass ich verzichten muss? Und dann wären wir wieder am Ende der Reisefreiheit wieder auf DDR-Status angekommen.

Können wir vielleicht danach noch mal diskutieren. Die Frage an die anderen drei Personen, ob sich was nach dieser heutigen Veranstaltung der Einstellung geändert hat.

Nicht wirklich. Vielleicht noch mal ein kurzer Einschnitt zum Thema Einstellung. Ich habe da ein paar mehr Informationen bekommen, was alles möglich ist, was ich auch erschreckend finde. Es ist auch immer eine zwiespältige Sache mit dem Datenschutz. Auf der einen Seite sind Daten notwendig und können auch sehr hilfreich sein, aber man muss eben aufpassen, dass das nicht so in die Privatsphäre hineingeht. Und ich möchte eben nicht komplett durchleuchtet werden und dann von allen irgendwie erkannt werden. Das möchte ich einfach nicht.

Das wäre jetzt der neunte Punkt, dass jeder vielleicht noch mal ein Statement abgibt. Das war ja dann schon das erste. Dass wir dann einfach noch mal rum gehen und jeder für sich noch mal zusammenfasst.

Das Datenschutzgesetz besteht ja schon seit den 80er Jahren, es ist also für mich persönlich nichts Neues. Ich weiß, welche Möglichkeiten ich habe Daten zu überprüfen, ich weiß, wie ich das machen kann. Ich weiß aber genauso, wie ich mich davor schützen kann, nur bin ich mir sicher, dass nicht alle wissen, dass sie das können und welche Möglichkeiten man hat. Ich wollte eigentlich immer mal wieder in die Staaten reisen, ich werde es nicht mehr tun, weil ich jetzt sogar schon 14 Tage vorher meine Daten über das Internet an eine bestimmte Stelle in Amerika melden muss. Und da wird dann auch noch, so wie es da steht, nach Krankheiten und sonstigen Dingen gefragt, Neigungen, und da geht es mit wirklich zu weit. Ich habe hin und wieder auch beruflich diese Fragestellung, gerade was Datenschutz angeht, wegen der Speicherung persönlicher Daten. Meine Einstellung hat sich heute gar nicht dazu geändert. Den Fragebogen haben Sie uns ja schon vorher geschickt. Und das war sehr harmlos, was Sie uns da gegeben haben. Szenarien, die ich in den nächsten Jahren sehe, sind noch wesentlich kritischer und zwar nicht die Technologie, sondern die Verknüpfung der Daten, die dahinterstehen. Da sehe ich große Gefahren, weil internationale Unternehmen großes Interesse an ihren persönlichen Informationen haben.

Dann frag ich da noch mal. Es kann auch ein kurzes und knackiges Statement sein.

Es hat sich auch bei mir nicht geändert. Es bleibt ein generelles Misstrauen gegenüber der Datensammlung und gegenüber Technologien, gleichzeitig manchmal im Allgemeinen Umgang mit der Gleichgültigkeit gepaart.

Ich hatte vorher schon eine recht kritische Einstellung zu der Datensammelwut, die unter unseren Politikern im Moment ausbricht. Das kann sich heute eigentlich nicht verschärft haben. Also, eine gleichbleibend negative Einstellung dazu. Auch sammelt die Wirtschaft zu viele Daten und muss schärfer kontrolliert werden.

Ich denke auch, das es diesbezüglich die Notwendigkeit gibt, dass eine Höchstdauer für Datensätze gibt oder dass es auch für Daten, die hier gesammelt werden und dann ins Ausland gebracht werden, gibt. Ich habe meine Meinung auch nicht verbessern können, sondern ich habe mittlerweile ein regelrechtes Misstrauen an den Tag gelegt, weil ich so viele Missbrauchsmöglichkeiten sehe, dass ich mir nicht vorstellen kann, dass die Versuchung nicht doch zu groß ist.

Die Veranstaltung heute hat meine Meinung nicht verändert, sondern verschärft. Die hat sich in der letzten Zeit ohnehin zu einer Besorgnis hin entwickelt. Ich lebe sonst unbeschwert, aber gerade diese neuen Entwicklungen, was die vermeintliche Sicherheit angeht, macht mit zunehmend Sorgen und ich finde es ganz schlimm, dass die Überprüfung aller Menschen darauf basiert, dass es eine ganz geringe Minderheit von Menschen diese Taten ausüben und darunter alle zu leiden haben. Die schwarzen Schafe sind maßgeblich dafür, wie wir alle in Zukunft behandelt werden. Das finde ich ist auch eine ganz falsche Einstellung zum Menschen.

Annex 6 - Frequency tables

Frequency Table

q1sex^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid male	13	61,9	61,9	61,9
female	8	38,1	38,1	100,0
Total	21	100,0	100,0	

a. country = DE

q2age^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 20	1	4,8	4,8	4,8
22	1	4,8	4,8	9,5
26	1	4,8	4,8	14,3
27	2	9,5	9,5	23,8
34	1	4,8	4,8	28,6
36	3	14,3	14,3	42,9
41	1	4,8	4,8	47,6
45	1	4,8	4,8	52,4
47	1	4,8	4,8	57,1
55	1	4,8	4,8	61,9
57	1	4,8	4,8	66,7
59	1	4,8	4,8	71,4
66	2	9,5	9,5	81,0
68	2	9,5	9,5	90,5
70	1	4,8	4,8	95,2
74	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q3household Persons in household ink self

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	10	47,6	47,6	47,6
2	8	38,1	38,1	85,7
3	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q4childrer^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid yes	9	42,9	42,9	42,9
no	12	57,1	57,1	100,0
Total	21	100,0	100,0	

a. country = DE

q5childhome1 No children^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	2	9,5	9,5	9,5
yes	19	90,5	90,5	100,0
Total	21	100,0	100,0	

a. country = DE

q5childhome2 14 or younger^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q5childhome3 15 or older^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q6edu^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 2	1	4,8	4,8	4,8
3	2	9,5	9,5	14,3
4	3	14,3	14,3	28,6
5	5	23,8	23,8	52,4
6	10	47,6	47,6	100,0
Total	21	100,0	100,0	

a. country = DE

q7occupstring^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Angestellte	2	9,5	9,5	9,5
Angestellter	2	9,5	9,5	19,0
Beamter	3	14,3	14,3	33,3
Geograph	1	4,8	4,8	38,1
IT-Admin.	1	4,8	4,8	42,9
Lehrerin	1	4,8	4,8	47,6
Meister	1	4,8	4,8	52,4
Musiker pp	1	4,8	4,8	57,1
Pensionärin	1	4,8	4,8	61,9
Rentner	2	9,5	9,5	71,4
Rentnerin	2	9,5	9,5	81,0
Student	3	14,3	14,3	95,2
Studentin	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q8district^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Metro	17	81,0	81,0	81,0
Provincial town	2	9,5	9,5	90,5
Rural	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q9phone^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	6	28,6	28,6	28,6
at least once a week	7	33,3	33,3	61,9
at least once a month	3	14,3	14,3	76,2
less than once a month	4	19,0	19,0	95,2
never	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q10email^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	8	38,1	38,1	38,1
at least once a week	10	47,6	47,6	85,7
at least once a month	1	4,8	4,8	90,5
less than once a month	1	4,8	4,8	95,2
never	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q11internet^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	13	61,9	61,9	61,9
at least once a week	5	23,8	23,8	85,7
at least once a month	2	9,5	9,5	95,2
never	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q12publictransport^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	3	14,3	14,3	14,3
at least once a week	3	14,3	14,3	28,6
at least once a month	8	38,1	38,1	66,7
less than once a month	7	33,3	33,3	100,0
Total	21	100,0	100,0	

a. country = DE

q13plane^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid more than 5 times a year	1	4,8	4,8	4,8
3-5 times a year	1	4,8	4,8	9,5
1-2 times a year	7	33,3	33,3	42,9
less than 1 time a year	11	52,4	52,4	95,2
never	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q14car^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	2	9,5	9,5	9,5
at least once a week	5	23,8	23,8	33,3
at least once a month	7	33,3	33,3	66,7
less than once a month	5	23,8	23,8	90,5
never	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q15general The security of society is absolutely dependent on the development and use of new security technologies

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	2	9,5	9,5	9,5
partly agree	8	38,1	38,1	47,6
partly disagree	7	33,3	33,3	81,0
completely disagree	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	8	38,1	38,1	38,1
partly agree	11	52,4	52,4	90,5
partly disagree	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	2	9,5	9,5	9,5
partly agree	5	23,8	23,8	33,3
partly disagree	3	14,3	14,3	47,6
completely disagree	11	52,4	52,4	100,0
Total	21	100,0	100,0	

a. country = DE

q18general When security technology is available, we might just as well make use of it

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	2	9,5	9,5	9,5
partly agree	7	33,3	33,3	42,9
partly disagree	5	23,8	23,8	66,7
completely disagree	7	33,3	33,3	100,0
Total	21	100,0	100,0	

a. country = DE

q19general Privacy should not be violated without reasonable suspicion of criminal intent

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	15	71,4	71,4	71,4
partly agree	5	23,8	23,8	95,2
neither agree nor disagree	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	13	61,9	61,9	61,9
partly agree	6	28,6	28,6	90,5
partly disagree	1	4,8	4,8	95,2
completely disagree	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q21general New security technologies are likely to be abused by governmental agencies^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	5	23,8	23,8	23,8
partly agree	8	38,1	38,1	61,9
neither agree nor disagree	4	19,0	19,0	81,0
partly disagree	1	4,8	4,8	85,7
completely disagree	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q22general New security technologies are likely to be abused by criminals^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	14	66,7	66,7	66,7
partly agree	7	33,3	33,3	100,0
Total	21	100,0	100,0	

a. country = DE

q23biom1 Facial characteristics^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	15	71,4	71,4	71,4
yes	6	28,6	28,6	100,0
Total	21	100,0	100,0	

a. country = DE

q23biom2 Fingerprints^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	16	76,2	76,2	76,2
yes	5	23,8	23,8	100,0
Total	21	100,0	100,0	

a. country = DE

q23biom3 Iris recognition^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	17	81,0	81,0	81,0
yes	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q23biom4 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	10	47,6	47,6	47,6
yes	11	52,4	52,4	100,0
Total	21	100,0	100,0	

a. country = DE

q23biom5 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom1 Bank^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	16	76,2	76,2	76,2
yes	5	23,8	23,8	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom2 Airport^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	10	47,6	47,6	47,6
yes	11	52,4	52,4	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom3 Store^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom4 Border^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	11	52,4	52,4	52,4
yes	10	47,6	47,6	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom5 Central bus and train station^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	16	76,2	76,2	76,2
yes	5	23,8	23,8	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom6 Stadium and crowded^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	16	76,2	76,2	76,2
yes	5	23,8	23,8	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom7 Other private service^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	17	81,0	81,0	81,0
yes	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom8 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	13	61,9	61,9	61,9
yes	8	38,1	38,1	100,0
Total	21	100,0	100,0	

a. country = DE

q24biom9 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q25biom Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	3	14,3	14,3	14,3
partly agree	3	14,3	14,3	28,6
neither agree nor disagree	2	9,5	9,5	38,1
partly disagree	1	4,8	4,8	42,9
completely disagree	12	57,1	57,1	100,0
Total	21	100,0	100,0	

a. country = DE

q26biom The use of the biometric passport makes me feel insecure because of the risk of my biometric data being stolen

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	8	38,1	38,1	38,1
partly agree	6	28,6	28,6	66,7
neither agree nor disagree	4	19,0	19,0	85,7
partly disagree	1	4,8	4,8	90,5
completely disagree	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q27visual1 Store^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	13	61,9	61,9	61,9
yes	8	38,1	38,1	100,0
Total	21	100,0	100,0	

a. country = DE

q27visual2 Dressing room^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q27visual3 Central bus and train station^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	10	47,6	47,6	47,6
yes	11	52,4	52,4	100,0
Total	21	100,0	100,0	

a. country = DE

q27visual4 Bank^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	5	23,8	23,8	23,8
yes	16	76,2	76,2	100,0
Total	21	100,0	100,0	

a. country = DE

q27visual5 Airport^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	5	23,8	23,8	23,8
yes	16	76,2	76,2	100,0
Total	21	100,0	100,0	

a. country = DE

q27visual6 Stadium and crowded

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	38,1	38,1	38,1
	yes	13	61,9	61,9	100,0
	Total	21	100,0	100,0	

a. country = DE

q27visual7 All public

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	81,0	81,0	81,0
	yes	4	19,0	19,0	100,0
	Total	21	100,0	100,0	

a. country = DE

q27visual8 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	95,2	95,2	95,2
	yes	1	4,8	4,8	100,0
	Total	21	100,0	100,0	

a. country = DE

q27visual9 d.k.^a

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	95,2	95,2	95,2
	yes	1	4,8	4,8	100,0
	Total	21	100,0	100,0	

a. country = DE

q28visual How do you feel about the number of CCTV cameras in public spaces in general?

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid there should be more	2	9,5	11,8	11,8
the number is appropriate	6	28,6	35,3	47,1
there should be less	3	14,3	17,6	64,7
there should be no	6	28,6	35,3	100,0
Total	17	81,0	100,0	
Missing d.k.	4	19,0		
Total	21	100,0		

a. country = DE

q29visual1 School

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q29visual2 Central bus and train station

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	16	76,2	76,2	76,2
yes	5	23,8	23,8	100,0
Total	21	100,0	100,0	

a. country = DE

q29visual3 Airport

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	3	14,3	14,3	14,3
yes	18	85,7	85,7	100,0
Total	21	100,0	100,0	

a. country = DE

q29visual4 Shopping mall^a

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	95,2	95,2	95,2
	yes	1	4,8	4,8	100,0
	Total	21	100,0	100,0	

a. country = DE

q29visual5 Public buildings^a

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	85,7	85,7	85,7
	yes	3	14,3	14,3	100,0
	Total	21	100,0	100,0	

a. country = DE

q29visual6 Never^a

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	100,0	100,0	100,0

a. country = DE

q29visual7 d.k.^a

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	95,2	100,0	100,0
Missing	System	1	4,8		
Total		21	100,0		

a. country = DE

q30visual1 Reveal everything^a

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	100,0	100,0	100,0

a. country = DE

q30visual2 Mannequin projection^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	8	38,1	38,1	38,1
yes	13	61,9	61,9	100,0
Total	21	100,0	100,0	

a. country = DE

q30visual3 Body heat, sweat & heart rate^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q30visual4 Meta^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	8	38,1	38,1	38,1
yes	13	61,9	61,9	100,0
Total	21	100,0	100,0	

a. country = DE

q30visual5 Luggage x-ray^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	6	28,6	28,6	28,6
yes	15	71,4	71,4	100,0
Total	21	100,0	100,0	

a. country = DE

q30visual6 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q30visual7 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q31visual CCTV surveillance makes me feel more secure^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	2	9,5	9,5	9,5
partly agree	10	47,6	47,6	57,1
neither agree nor disagree	1	4,8	4,8	61,9
partly disagree	2	9,5	9,5	71,4
completely disagree	6	28,6	28,6	100,0
Total	21	100,0	100,0	

a. country = DE

q32visual CCTV surveillance infringes my privacy^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	8	38,1	38,1	38,1
partly agree	6	28,6	28,6	66,7
neither agree nor disagree	1	4,8	4,8	71,4
partly disagree	3	14,3	14,3	85,7
completely disagree	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q33visual Scanning of persons for detection of hidden items is an acceptable tool for preventing terror^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	6	28,6	28,6	28,6
partly agree	7	33,3	33,3	61,9
partly disagree	5	23,8	23,8	85,7
completely disagree	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q34local1 Terrorists and criminals w court order^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	3	14,3	14,3	14,3
yes	18	85,7	85,7	100,0
Total	21	100,0	100,0	

a. country = DE

q34local2 Any w/o court order^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q34local3 Emergency^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	2	9,5	9,5	9,5
yes	19	90,5	90,5	100,0
Total	21	100,0	100,0	

a. country = DE

q34local4 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q34local5 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q35local1 Terrorists and criminals w court order^f

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	3	14,3	14,3	14,3
yes	18	85,7	85,7	100,0
Total	21	100,0	100,0	

a. country = DE

q35local2 Any w/o court order^f

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q35local3 Stolen vehicles^g

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	10	47,6	47,6	47,6
yes	11	52,4	52,4	100,0
Total	21	100,0	100,0	

a. country = DE

q35local4 Speeding^f

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q35local5 Automatic accident reporting^g

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	7	33,3	33,3	33,3
yes	14	66,7	66,7	100,0
Total	21	100,0	100,0	

a. country = DE

q35local6 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q35local7 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q36local Should eCall automatically be installed in all new cars?

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid yes	4	19,0	19,0	19,0
yes but possible to deactivate	2	9,5	9,5	28,6
no, optional	11	52,4	52,4	81,0
no, never	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q37local The possibility of locating all mobile phones is privacy infringing

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	14	66,7	66,7	66,7
partly agree	4	19,0	19,0	85,7
neither agree nor disagree	1	4,8	4,8	90,5
completely disagree	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q38local The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	5	23,8	23,8	23,8
partly agree	9	42,9	42,9	66,7
neither agree nor disagree	1	4,8	4,8	71,4
partly disagree	3	14,3	14,3	85,7
completely disagree	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q39local The possibility of locating all cars is privacy infringing

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	15	71,4	71,4	71,4
partly agree	4	19,0	19,0	90,5
completely disagree	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

40local The possibility of locating all cars is a good tool for the police in investigating and preventing terror and crime

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	4	19,0	19,0	19,0
partly agree	8	38,1	38,1	57,1
neither agree nor disagree	1	4,8	4,8	61,9
partly disagree	3	14,3	14,3	76,2
completely disagree	5	23,8	23,8	100,0
Total	21	100,0	100,0	

a. country = DE

q41data1 Prevention of terrorism

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	13	61,9	61,9	61,9
yes	8	38,1	38,1	100,0
Total	21	100,0	100,0	

a. country = DE

q41data2 Investigation of terrorism^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	9	42,9	42,9	42,9
yes	12	57,1	57,1	100,0
Total	21	100,0	100,0	

a. country = DE

q41data3 Prevention of crime^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	18	85,7	85,7	85,7
yes	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q41data4 Investigation of crime^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	11	52,4	52,4	52,4
yes	10	47,6	47,6	100,0
Total	21	100,0	100,0	

a. country = DE

q41data5 Commercial^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q41data6 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	13	61,9	61,9	61,9
yes	8	38,1	38,1	100,0
Total	21	100,0	100,0	

a. country = DE

q41data7 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q42data1 Prevention of terrorism^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	14	66,7	66,7	66,7
yes	7	33,3	33,3	100,0
Total	21	100,0	100,0	

a. country = DE

q42data2 Investigation of terrorism^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	8	38,1	38,1	38,1
yes	13	61,9	61,9	100,0
Total	21	100,0	100,0	

a. country = DE

q42data3 Prevention of crime^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	16	76,2	76,2	76,2
yes	5	23,8	23,8	100,0
Total	21	100,0	100,0	

a. country = DE

q42data4 Investigation of crime^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	7	33,3	33,3	33,3
yes	14	66,7	66,7	100,0
Total	21	100,0	100,0	

a. country = DE

q42data5 Commercial^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q42data6 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	15	71,4	71,4	71,4
yes	6	28,6	28,6	100,0
Total	21	100,0	100,0	

a. country = DE

q42data7 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	1	4,8	4,8	4,8
partly agree	4	19,0	19,0	23,8
neither agree nor disagree	2	9,5	9,5	33,3
partly disagree	5	23,8	23,8	57,1
completely disagree	9	42,9	42,9	100,0
Total	21	100,0	100,0	

a. country = DE

q44data Data from phone, mobile and Internet communication_a should not be stored beyond what is needed for billing purposes

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	15	71,4	71,4	71,4
partly agree	2	9,5	9,5	81,0
partly disagree	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q45data Scanning of and combining data from different databases containing personal information is privacy infringing

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	17	81,0	81,0	81,0
partly agree	2	9,5	9,5	90,5
partly disagree	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q46data Scanning of and combining data from different databases is a good tool for police to prevent terror

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	5	23,8	23,8	23,8
partly agree	6	28,6	28,6	52,4
neither agree nor disagree	1	4,8	4,8	57,1
partly disagree	2	9,5	9,5	66,7
completely disagree	7	33,3	33,3	100,0
Total	21	100,0	100,0	

a. country = DE

q47data Databases being used for something else than the original purpose is a serious privacy problem

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	20	95,2	95,2	95,2
partly agree	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q48wire1 Prevention and investigation of terrorism w court order^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	4	19,0	19,0	19,0
yes	17	81,0	81,0	100,0
Total	21	100,0	100,0	

a. country = DE

q48wire2 Prevention and investigation of terrorism w/o court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q48wire3 Prevention and investigation of crime w court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	2	9,5	9,5	9,5
yes	19	90,5	90,5	100,0
Total	21	100,0	100,0	

a. country = DE

q48wire4 Prevention and investigation of crime w/o court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q48wire5 Commercial^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q48wire6 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q48wire7 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q49wire What methods of eavesdropping is acceptable?

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid all communication lines	3	14,3	14,3	14,3
persons that suspect is expected to contact	3	14,3	14,3	28,6
suspects	11	52,4	52,4	81,0
totally unacceptable	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q50wire Eavesdropping is a good tool for police investigation^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	7	33,3	33,3	33,3
partly agree	6	28,6	28,6	61,9
partly disagree	4	19,0	19,0	81,0
completely disagree	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q51wire Eavesdropping is a serious violation of privacy

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	17	81,0	81,0	81,0
partly agree	3	14,3	14,3	95,2
partly disagree	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q52protect1 Anonymous calling card

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	8	38,1	38,1	38,1
yes	13	61,9	61,9	100,0
Total	21	100,0	100,0	

a. country = DE

q52protect2 Encryption programme

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	6	28,6	28,6	28,6
yes	15	71,4	71,4	100,0
Total	21	100,0	100,0	

a. country = DE

q52protect3 Identity management

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	8	38,1	38,1	38,1
yes	13	61,9	61,9	100,0
Total	21	100,0	100,0	

a. country = DE

q52protect4 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	18	85,7	85,7	85,7
yes	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q52protect5 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	11	52,4	52,4	52,4
partly agree	5	23,8	23,8	76,2
neither agree nor disagree	2	9,5	9,5	85,7
partly disagree	1	4,8	4,8	90,5
completely disagree	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q54protect Privacy enhancing technologies should not be legal if they make police investigation and prevention of terror and crime more difficult

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	4	19,0	19,0	19,0
partly agree	1	4,8	4,8	23,8
neither agree nor disagree	2	9,5	9,5	33,3
partly disagree	4	19,0	19,0	52,4
completely disagree	10	47,6	47,6	100,0
Total	21	100,0	100,0	

a. country = DE

q55dilem1 Accept registration of travel and fingerprints

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q55dilem2 Accept only if template^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q55dilem3 Accept only if deleted^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	13	61,9	61,9	61,9
yes	8	38,1	38,1	100,0
Total	21	100,0	100,0	

a. country = DE

q55dilem4 Accept only if not exclusive^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	10	47,6	47,6	47,6
yes	11	52,4	52,4	100,0
Total	21	100,0	100,0	

a. country = DE

q55dilem5 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	9	42,9	42,9	42,9
yes	12	57,1	57,1	100,0
Total	21	100,0	100,0	

a. country = DE

q55dilem6 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q56dilem1 Accept database and biometric^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	16	76,2	76,2	76,2
yes	5	23,8	23,8	100,0
Total	21	100,0	100,0	

a. country = DE

q56dilem2 Accept naked machine^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	17	81,0	81,0	81,0
yes	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q56dilem3 Accept sweat, body heat and heart rate scanning^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q56dilem4 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	9	42,9	42,9	42,9
yes	12	57,1	57,1	100,0
Total	21	100,0	100,0	

a. country = DE

q56dilem5 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q57dilem1 Accept all consequences^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q57dilem2 Accept only low rate of false positives^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q57dilem3 Accept only no false positives^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	11	52,4	52,4	52,4
yes	10	47,6	47,6	100,0
Total	21	100,0	100,0	

a. country = DE

q57dilem4 Accept only in exposed places^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	12	57,1	57,1	57,1
yes	9	42,9	42,9	100,0
Total	21	100,0	100,0	

a. country = DE

q57dilem5 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	14	66,7	66,7	66,7
yes	7	33,3	33,3	100,0
Total	21	100,0	100,0	

a. country = DE

q57dilem6 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q58dilem1 Accept all access for counter terrorism

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q58dilem2 Accept only if anonymous and w court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	5	23,8	23,8	23,8
yes	16	76,2	76,2	100,0
Total	21	100,0	100,0	

a. country = DE

q58dilem3 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	17	81,0	81,0	81,0
yes	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q58dilem4 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q59dilem1 Accept locate car to prevent crime or terrorism¹

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	13	61,9	61,9	61,9
yes	8	38,1	38,1	100,0
Total	21	100,0	100,0	

a. country = DE

q59dilem2 Accept speeding tickets²

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	90,5	90,5	90,5
yes	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q59dilem3 Accept register all movements³

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q59dilem4 Accept only accidents⁴

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	9	42,9	42,9	42,9
yes	12	57,1	57,1	100,0
Total	21	100,0	100,0	

a. country = DE

q59dilem5 Accept only if voluntary⁵

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	6	28,6	28,6	28,6
yes	15	71,4	71,4	100,0
Total	21	100,0	100,0	

a. country = DE

q59dilem6 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q60dilem1 Accept calling cards[§]

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	7	33,3	33,3	33,3
yes	14	66,7	66,7	100,0
Total	21	100,0	100,0	

a. country = DE

q60dilem2 Accept encryption[¶]

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	7	33,3	33,3	33,3
yes	14	66,7	66,7	100,0
Total	21	100,0	100,0	

a. country = DE

q60dilem3 Accept Internet anonymity - bomb[§]

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	12	57,1	57,1	57,1
yes	9	42,9	42,9	100,0
Total	21	100,0	100,0	

a. country = DE

q60dilem4 Accept Internet anonymity - child pornography[¶]

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	14	66,7	66,7	66,7
yes	7	33,3	33,3	100,0
Total	21	100,0	100,0	

a. country = DE

q60dilem5 Never^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	18	85,7	85,7	85,7
yes	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q60dilem6 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q61dilem1 Accept exclusion of refusers from public service^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	17	81,0	81,0	81,0
yes	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q61dilem2 Accept exclusion of unabled from public service^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q61dilem3 Accept refusers are impended when public transport^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	13	61,9	61,9	61,9
yes	8	38,1	38,1	100,0
Total	21	100,0	100,0	

a. country = DE

q61dilem4 Accept unable are impended when public transport

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	95,2	95,2	95,2
yes	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q61dilem5 Accept no consequences for refusers

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	9	42,9	42,9	42,9
yes	12	57,1	57,1	100,0
Total	21	100,0	100,0	

a. country = DE

q61dilem6 Accept no consequences for unable

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	9	42,9	42,9	42,9
yes	12	57,1	57,1	100,0
Total	21	100,0	100,0	

a. country = DE

q61dilem7 d.k.^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	100,0	100,0	100,0

a. country = DE

q62demo Politicians must always submit important questions to public debate an public hearings before making decisions on implementing new security technologies^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	16	76,2	76,2	76,2
partly agree	2	9,5	9,5	85,7
partly disagree	3	14,3	14,3	100,0
Total	21	100,0	100,0	

a. country = DE

q63demo The subject of security and privacy is so complicated that it makes no sense to include the general public in discussions of this issue

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	1	4,8	4,8	4,8
partly agree	3	14,3	14,3	19,0
neither agree nor disagree	1	4,8	4,8	23,8
partly disagree	2	9,5	9,5	33,3
completely disagree	14	66,7	66,7	100,0
Total	21	100,0	100,0	

a. country = DE

q64demo Human rights organisations are always entitled to be heard when important decisions on security and privacy are made

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	14	66,7	66,7	66,7
partly agree	6	28,6	28,6	95,2
neither agree nor disagree	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q65demo It is important that private companies involved in producing security technologies are also entitled to be heard when important decisions on security and privacy are made

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	7	33,3	33,3	33,3
partly agree	5	23,8	23,8	57,1
neither agree nor disagree	1	4,8	4,8	61,9
partly disagree	4	19,0	19,0	81,0
completely disagree	4	19,0	19,0	100,0
Total	21	100,0	100,0	

a. country = DE

q66demo In relation to significant decisions on the use of security technologies, it is imperative that alternative solutions are elucidated and included in the debate

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	19	90,5	90,5	90,5
neither agree nor disagree	2	9,5	9,5	100,0
Total	21	100,0	100,0	

a. country = DE

q67suggest Collection of personal data from unsuspecting individuals must be anonymous until identification is authorized by court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid high importance	16	76,2	80,0	80,0
some importance	3	14,3	15,0	95,0
little importance	1	4,8	5,0	100,0
Total	20	95,2	100,0	
Missing 99	1	4,8		
Total	21	100,0		

a. country = DE

q68suggest Only authorized personnel can have access to collected personal data

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid high importance	20	95,2	100,0	100,0
Missing 99	1	4,8		
Total	21	100,0		

a. country = DE

q69suggest Prior to implementing, new security technologies must be checked for privacy impact

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid high importance	17	81,0	85,0	85,0
some importance	3	14,3	15,0	100,0
Total	20	95,2	100,0	
Missing d.k.	1	4,8		
Total	21	100,0		

a. country = DE

q70suggest Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid high importance	10	47,6	47,6	47,6
some importance	5	23,8	23,8	71,4
little importance	5	23,8	23,8	95,2
not important at all	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

q71end Have you changed your attitude towards security technologies in general in the course of completing this questionnaire?

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid yes, more positive	1	4,8	5,0	5,0
yes, more worried	1	4,8	5,0	10,0
no	18	85,7	90,0	100,0
Total	20	95,2	100,0	
Missing d.k.	1	4,8		
Total	21	100,0		

a. country = DE

q72endstring^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	10	47,6	47,6	47,6
Videoaufzeichnungen akzeptabel wenn DS beachtet wird	1	4,8	4,8	52,4
Einige Antwortmöglichkeiten zu unscharf	1	4,8	4,8	57,1
Fehleranfälligkeit von Computersystemen bei Zusammenführung großer Datenmengen berücksichtigen	1	4,8	4,8	61,9
Fragen stark staatslastig	1	4,8	4,8	66,7
Kriminalisierung der Bürger	1	4,8	4,8	71,4
Neue Sicherheitstechnologien entwickeln, Terrorismus keinen technologischen Vorsprung lassen	1	4,8	4,8	76,2
Sicherheitstechnologie im Notfall nutzen, Angst vor Missbrauch	1	4,8	4,8	81,0
Sicherheitstechnologie macht Debatte nach Frieden teilweise sinnlos	1	4,8	4,8	85,7
Sicherheitstechnologien sind nicht nur Internet, Scanner, Video	1	4,8	4,8	90,5
Sicherheitstechnologien werden immer missbraucht werden können	1	4,8	4,8	95,2
Technikentwicklung nicht um jeden Preis, Gesellschaft nicht aus den Augen verlieren, Kriminalitätsursachen bekämpfen	1	4,8	4,8	100,0
Total	21	100,0	100,0	

a. country = DE

edu3^a

	Frequency	Percent
Missing System	21	100,0

a. country = DE

age3^a

	Frequency	Percent
Missing System	21	100,0

a. country = DE

edulSCED97^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid lower secondary level of education	1	4,8	4,8	4,8
upper secondary level of education	4	19,0	19,0	23,8
post-secondary non-tertiary	6	28,6	28,6	52,4
first stage of tertiary education	10	47,6	47,6	100,0
Total	21	100,0	100,0	

a. country = DE

edulSCED97binary Tertiary^a

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Shorter than tertiary	11	52,4	52,4	52,4
Tertiary	10	47,6	47,6	100,0
Total	21	100,0	100,0	

a. country = DE

AgeBinary Age over and under 50

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 18-49	12	57,1	57,1	57,1
50+	9	42,9	42,9	100,0
Total	21	100,0	100,0	

a. country = DE

Crosstabs 1

country = DE

q15general The security of society is absolutely dependent on the development and use of new security technologies * q1sex Crosstabulation^a

			q1sex		Total
			male	female	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	2	0	2
		% within q1sex	15,4%	,0%	9,5%
	partly agree	Count	4	4	8
		% within q1sex	30,8%	50,0%	38,1%
	partly disagree	Count	5	2	7
		% within q1sex	38,5%	25,0%	33,3%
	completely disagree	Count	2	2	4
		% within q1sex	15,4%	25,0%	19,0%
Total	Count	13	8	21	
	% within q1sex	100,0%	100,0%	100,0%	

a. country = DE

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q1sex Crosstabulation

				q1sex		Total
				male	female	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	4	4	8	
		% within q1sex	30,8%	50,0%	38,1%	
	partly agree	Count	9	2	11	
		% within q1sex	69,2%	25,0%	52,4%	
	partly disagree	Count	0	2	2	
		% within q1sex	,0%	25,0%	9,5%	
Total	Count	13	8	21		
	% within q1sex	100,0%	100,0%	100,0%		

a. country = DE

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * q1sex Crosstabulation

			q1sex		Total
			male	female	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	2	0	2
		% within q1sex	15,4%	,0%	9,5%
	partly agree	Count	2	3	5
		% within q1sex	15,4%	37,5%	23,8%
	partly disagree	Count	3	0	3
		% within q1sex	23,1%	,0%	14,3%
	completely disagree	Count	6	5	11
		% within q1sex	46,2%	62,5%	52,4%
Total	Count	13	8	21	
	% within q1sex	100,0%	100,0%	100,0%	

a. country = DE

q18general When security technology is available, we might just as well make use of it * q1sex Crosstabulation

			q1sex		Total
			male	female	
q18general When security technology is available, we might just as well make use of it	completely agree	Count	1	1	2
		% within q1sex	7,7%	12,5%	9,5%
	partly agree	Count	3	4	7
		% within q1sex	23,1%	50,0%	33,3%
	partly disagree	Count	4	1	5
		% within q1sex	30,8%	12,5%	23,8%
	completely disagree	Count	5	2	7
		% within q1sex	38,5%	25,0%	33,3%
Total	Count	13	8	21	
	% within q1sex	100,0%	100,0%	100,0%	

a. country = DE

19general Privacy should not be violated without reasonable suspicion of criminal intent * q1sex^a
Crosstabulation

			q1sex		Total
			male	female	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	8	7	15
		% within q1sex	61,5%	87,5%	71,4%
	partly agree	Count	5	0	5
		% within q1sex	38,5%	,0%	23,8%
	neither agree nor disagree	Count	0	1	1
		% within q1sex	,0%	12,5%	4,8%
Total	Count	13	8	21	
	% within q1sex	100,0%	100,0%	100,0%	

a. country = DE

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q1sex Crosstabulation^a

			q1sex		Total
			male	female	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	8	5	13
		% within q1sex	61,5%	62,5%	61,9%
	partly agree	Count	4	2	6
		% within q1sex	30,8%	25,0%	28,6%
	partly disagree	Count	0	1	1
		% within q1sex	,0%	12,5%	4,8%
	completely disagree	Count	1	0	1
		% within q1sex	7,7%	,0%	4,8%
Total	Count	13	8	21	
	% within q1sex	100,0%	100,0%	100,0%	

a. country = DE

q21general New security technologies are likely to be abused by governmental agencies * q1sex Crosstabulation

			q1sex		Total
			male	female	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	2	3	5
		% within q1sex	15,4%	37,5%	23,8%
	partly agree	Count	4	4	8
		% within q1sex	30,8%	50,0%	38,1%
	neither agree nor disagree	Count	4	0	4
		% within q1sex	30,8%	,0%	19,0%
	partly disagree	Count	1	0	1
		% within q1sex	7,7%	,0%	4,8%
	completely disagree	Count	2	1	3
		% within q1sex	15,4%	12,5%	14,3%
Total	Count	13	8	21	
	% within q1sex	100,0%	100,0%	100,0%	

a. country = DE

q22general New security technologies are likely to be abused by criminals * q1sex Crosstabulation

				q1sex		Total
				male	female	
q22general New security technologies are likely to be abused by criminals	completely agree	Count	6	8	14	
		% within q1sex	46,2%	100,0%	66,7%	
	partly agree	Count	7	0	7	
		% within q1sex	53,8%	,0%	33,3%	
Total		Count	13	8	21	
		% within q1sex	100,0%	100,0%	100,0%	

a. country = DE

q15general The security of society is absolutely dependent on the development and use of new security technologies * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	0	2	2
		% within AgeBinary Age over and under 50	,0%	22,2%	9,5%
	partly agree	Count	3	5	8
		% within AgeBinary Age over and under 50	25,0%	55,6%	38,1%
	partly disagree	Count	5	2	7
		% within AgeBinary Age over and under 50	41,7%	22,2%	33,3%
	completely disagree	Count	4	0	4
		% within AgeBinary Age over and under 50	33,3%	,0%	19,0%
Total		Count	12	9	21
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = DE

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * AgeBinary Age over and under 50 Crosstabulation

				AgeBinary Age over and under 50		Total
				18-49	50+	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	4	4	8	
		% within AgeBinary Age over and under 50	33,3%	44,4%	38,1%	
	partly agree	Count	7	4	11	
		% within AgeBinary Age over and under 50	58,3%	44,4%	52,4%	
	partly disagree	Count	1	1	2	
		% within AgeBinary Age over and under 50	8,3%	11,1%	9,5%	
Total		Count	12	9	21	
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%	

a. country = DE

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * AgeBinary Age over and under 50 Crosstabulation^a

			AgeBinary Age over and under 50		Total
			18-49	50+	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	1	1	2
		% within AgeBinary Age over and under 50	8,3%	11,1%	9,5%
	partly agree	Count	1	4	5
		% within AgeBinary Age over and under 50	8,3%	44,4%	23,8%
	partly disagree	Count	2	1	3
		% within AgeBinary Age over and under 50	16,7%	11,1%	14,3%
	completely disagree	Count	8	3	11
		% within AgeBinary Age over and under 50	66,7%	33,3%	52,4%
Total		Count	12	9	21
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = DE

q18general When security technology is available, we might just as well make use of it * AgeBinary Age over and under 50 Crosstabulation^a

			AgeBinary Age over and under 50		Total
			18-49	50+	
q18general When security technology is available, we might just as well make use of it	completely agree	Count	0	2	2
		% within AgeBinary Age over and under 50	,0%	22,2%	9,5%
	partly agree	Count	3	4	7
		% within AgeBinary Age over and under 50	25,0%	44,4%	33,3%
	partly disagree	Count	4	1	5
		% within AgeBinary Age over and under 50	33,3%	11,1%	23,8%
	completely disagree	Count	5	2	7
		% within AgeBinary Age over and under 50	41,7%	22,2%	33,3%
Total		Count	12	9	21
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = DE

**q19general Privacy should not be violated without reasonable suspicion of criminal intent * AgeBinary
Age over and under 50 Crosstabulation**

			AgeBinary Age over and under 50		Total
			18-49	50+	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	9	6	15
		% within AgeBinary Age over and under 50	75,0%	66,7%	71,4%
	partly agree	Count	3	2	5
		% within AgeBinary Age over and under 50	25,0%	22,2%	23,8%
	neither agree nor disagree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	11,1%	4,8%
Total	Count	12	9	21	
	% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%	

a. country = DE

**q20general It is uncomfortable to be under surveillance, even though you have no criminal intent *
AgeBinary Age over and under 50 Crosstabulation**

			AgeBinary Age over and under 50		Total
			18-49	50+	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	8	5	13
		% within AgeBinary Age over and under 50	66,7%	55,6%	61,9%
	partly agree	Count	2	4	6
		% within AgeBinary Age over and under 50	16,7%	44,4%	28,6%
	partly disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	8,3%	,0%	4,8%
	completely disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	8,3%	,0%	4,8%
Total		Count	12	9	21
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = DE

**q21general New security technologies are likely to be abused by governmental agencies * AgeBinary
Age over and under 50 Crosstabulation^a**

Age			AgeBinary Age over and under 50		Total
			18-49	50+	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	3	2	5
		% within AgeBinary Age over and under 50	25,0%	22,2%	23,8%
	partly agree	Count	4	4	8
		% within AgeBinary Age over and under 50	33,3%	44,4%	38,1%
	neither agree nor disagree	Count	3	1	4
		% within AgeBinary Age over and under 50	25,0%	11,1%	19,0%
	partly disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	8,3%	,0%	4,8%
	completely disagree	Count	1	2	3
		% within AgeBinary Age over and under 50	8,3%	22,2%	14,3%
Total		Count	12	9	21
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

a. country = DE

**q22general New security technologies are likely to be abused by criminals * AgeBinary Age over
and under 50 Crosstabulation^a**

				AgeBinary Age over and under 50		Total
				18-49	50+	
q22general New security technologies are likely to be abused by criminals	completely agree	Count		8	6	14
		% within AgeBinary Age over and under 50		66,7%	66,7%	66,7%
	partly agree	Count		4	3	7
		% within AgeBinary Age over and under 50		33,3%	33,3%	33,3%
Total		Count		12	9	21
		% within AgeBinary Age over and under 50		100,0%	100,0%	100,0%

a. country = DE

q15general The security of society is absolutely dependent on the development and use of new security technologies * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count % within eduISCED97binary Tertiary	1 9,1%	1 10,0%	2 9,5%
	partly agree	Count % within eduISCED97binary Tertiary	4 36,4%	4 40,0%	8 38,1%
	partly disagree	Count % within eduISCED97binary Tertiary	3 27,3%	4 40,0%	7 33,3%
	completely disagree	Count % within eduISCED97binary Tertiary	3 27,3%	1 10,0%	4 19,0%
Total		Count % within eduISCED97binary Tertiary	11 100,0%	10 100,0%	21 100,0%

a. country = DE

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count % within eduISCED97binary Tertiary	6 54,5%	2 20,0%	8 38,1%
	partly agree	Count % within eduISCED97binary Tertiary	4 36,4%	7 70,0%	11 52,4%
	partly disagree	Count % within eduISCED97binary Tertiary	1 9,1%	1 10,0%	2 9,5%
Total		Count % within eduISCED97binary Tertiary	11 100,0%	10 100,0%	21 100,0%

a. country = DE

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * eduISCED97binary Tertiary Crosstabulation^a

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count % within eduISCED97binary Tertiary	1 9,1%	1 10,0%	2 9,5%
	partly agree	Count % within eduISCED97binary Tertiary	2 18,2%	3 30,0%	5 23,8%
	partly disagree	Count % within eduISCED97binary Tertiary	0 ,0%	3 30,0%	3 14,3%
	completely disagree	Count % within eduISCED97binary Tertiary	8 72,7%	3 30,0%	11 52,4%
Total		Count % within eduISCED97binary Tertiary	11 100,0%	10 100,0%	21 100,0%

a. country = DE

q18general When security technology is available, we might just as well make use of it * eduISCED97binary
Tertiary Crosstabulation

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q18general When security technology is available, we might just as well make use of it	completely agree	Count % within eduISCED97binary Tertiary	1 9,1%	1 10,0%	2 9,5%
	partly agree	Count % within eduISCED97binary Tertiary	5 45,5%	2 20,0%	7 33,3%
	partly disagree	Count % within eduISCED97binary Tertiary	1 9,1%	4 40,0%	5 23,8%
	completely disagree	Count % within eduISCED97binary Tertiary	4 36,4%	3 30,0%	7 33,3%
Total		Count % within eduISCED97binary Tertiary	11 100,0%	10 100,0%	21 100,0%

a. country = DE

q19general Privacy should not be violated without reasonable suspicion of criminal intent *
edulSCED97binary Tertiary Crosstabulation

			edulSCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count % within edulSCED97binary Tertiary	8 72,7%	7 70,0%	15 71,4%
	partly agree	Count % within edulSCED97binary Tertiary	3 27,3%	2 20,0%	5 23,8%
	neither agree nor disagree	Count % within edulSCED97binary Tertiary	0 ,0%	1 10,0%	1 4,8%
Total		Count % within edulSCED97binary Tertiary	11 100,0%	10 100,0%	21 100,0%

a. country = DE

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent *
eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count % within eduISCED97binary Tertiary	10 90,9%	3 30,0%	13 61,9%
	partly agree	Count % within eduISCED97binary Tertiary	0 ,0%	6 60,0%	6 28,6%
	partly disagree	Count % within eduISCED97binary Tertiary	1 9,1%	0 ,0%	1 4,8%
	completely disagree	Count % within eduISCED97binary Tertiary	0 ,0%	1 10,0%	1 4,8%
Total		Count % within eduISCED97binary Tertiary	11 100,0%	10 100,0%	21 100,0%

a. country = DE

q21general New security technologies are likely to be abused by governmental agencies *
eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count % within eduISCED97binary Tertiary	4 36,4%	1 10,0%	5 23,8%
	partly agree	Count % within eduISCED97binary Tertiary	6 54,5%	2 20,0%	8 38,1%
	neither agree nor disagree	Count % within eduISCED97binary Tertiary	1 9,1%	3 30,0%	4 19,0%
	partly disagree	Count % within eduISCED97binary Tertiary	0 ,0%	1 10,0%	1 4,8%
	completely disagree	Count % within eduISCED97binary Tertiary	0 ,0%	3 30,0%	3 14,3%
Total		Count % within eduISCED97binary Tertiary	11 100,0%	10 100,0%	21 100,0%

a. country = DE

q22general New security technologies are likely to be abused by criminals * eduISCED97binary Tertiary Crosstabulation^a

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q22general New security technologies are likely to be abused by criminals	completely agree	Count % within eduISCED97binary Tertiary	9 81,8%	5 50,0%	14 66,7%
	partly agree	Count % within eduISCED97binary Tertiary	2 18,2%	5 50,0%	7 33,3%
Total		Count % within eduISCED97binary Tertiary	11 100,0%	10 100,0%	21 100,0%

a. country = DE

q15general The security of society is absolutely dependent on the development and use of new security technologies * q4children Crosstabulation^a

			q4children		Total
			yes	no	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	2	0	2
		% within q4children	22,2%	,0%	9,5%
	partly agree	Count	5	3	8
		% within q4children	55,6%	25,0%	38,1%
	partly disagree	Count	2	5	7
		% within q4children	22,2%	41,7%	33,3%
	completely disagree	Count	0	4	4
		% within q4children	,0%	33,3%	19,0%
Total	Count	9	12	21	
	% within q4children	100,0%	100,0%	100,0%	

a. country = DE

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q4children Crosstabulation

				q4children		Total
				yes	no	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	4	4	8	
		% within q4children	44,4%	33,3%	38,1%	
	partly agree	Count	5	6	11	
		% within q4children	55,6%	50,0%	52,4%	
	partly disagree	Count	0	2	2	
		% within q4children	,0%	16,7%	9,5%	
Total	Count	9	12	21		
	% within q4children	100,0%	100,0%	100,0%		

a. country = DE

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * q4children Crosstabulation

			q4children		Total
			yes	no	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	1	1	2
		% within q4children	11,1%	8,3%	9,5%
	partly agree	Count	3	2	5
		% within q4children	33,3%	16,7%	23,8%
	partly disagree	Count	2	1	3
		% within q4children	22,2%	8,3%	14,3%
	completely disagree	Count	3	8	11
		% within q4children	33,3%	66,7%	52,4%
Total	Count	9	12	21	
	% within q4children	100,0%	100,0%	100,0%	

a. country = DE

q18general When security technology is available, we might just as well make use of it * q4children Crosstabulation

			q4children		Total
			yes	no	
q18general When security technology is available, we might just as well make use of it	completely agree	Count	2	0	2
		% within q4children	22,2%	,0%	9,5%
	partly agree	Count	3	4	7
		% within q4children	33,3%	33,3%	33,3%
	partly disagree	Count	2	3	5
		% within q4children	22,2%	25,0%	23,8%
	completely disagree	Count	2	5	7
		% within q4children	22,2%	41,7%	33,3%
Total	Count	9	12	21	
	% within q4children	100,0%	100,0%	100,0%	

a. country = DE

19general Privacy should not be violated without reasonable suspicion of criminal intent * q4children^a
Crosstabulation

			q4children		Total
			yes	no	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	7	8	15
		% within q4children	77,8%	66,7%	71,4%
	partly agree	Count	2	3	5
		% within q4children	22,2%	25,0%	23,8%
	neither agree nor disagree	Count	0	1	1
		% within q4children	,0%	8,3%	4,8%
Total	Count	9	12	21	
	% within q4children	100,0%	100,0%	100,0%	

a. country = DE

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent
*** q4children Crosstabulation^a**

			q4children		Total
			yes	no	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	6	7	13
		% within q4children	66,7%	58,3%	61,9%
	partly agree	Count	3	3	6
		% within q4children	33,3%	25,0%	28,6%
	partly disagree	Count	0	1	1
		% within q4children	,0%	8,3%	4,8%
	completely disagree	Count	0	1	1
		% within q4children	,0%	8,3%	4,8%
Total	Count	9	12	21	
	% within q4children	100,0%	100,0%	100,0%	

a. country = DE

q21general New security technologies are likely to be abused by governmental agencies * q4children Crosstabulation

			q4children		Total
			yes	no	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	2	3	5
		% within q4children	22,2%	25,0%	23,8%
	partly agree	Count	4	4	8
		% within q4children	44,4%	33,3%	38,1%
	neither agree nor disagree	Count	2	2	4
		% within q4children	22,2%	16,7%	19,0%
	partly disagree	Count	0	1	1
		% within q4children	,0%	8,3%	4,8%
	completely disagree	Count	1	2	3
		% within q4children	11,1%	16,7%	14,3%
Total	Count	9	12	21	
	% within q4children	100,0%	100,0%	100,0%	

a. country = DE

q22general New security technologies are likely to be abused by criminals * q4children Crosstabulation

				q4children		Total
				yes	no	
q22general New security technologies are likely to be abused by criminals	completely agree	Count	5	9	14	
		% within q4children	55,6%	75,0%	66,7%	
	partly agree	Count	4	3	7	
		% within q4children	44,4%	25,0%	33,3%	
Total		Count	9	12	21	
		% within q4children	100,0%	100,0%	100,0%	

a. country = DE

q15general The security of society is absolutely dependent on the development and use of new security technologies * q5childhome1 No children Crosstabulation^a

			q5childhome1 No children		Total
			no	yes	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count % within q5childhome1 No children	0 ,0%	2 10,5%	2 9,5%
	partly agree	Count % within q5childhome1 No children	2 100,0%	6 31,6%	8 38,1%
	partly disagree	Count % within q5childhome1 No children	0 ,0%	7 36,8%	7 33,3%
	completely disagree	Count % within q5childhome1 No children	0 ,0%	4 21,1%	4 19,0%
Total		Count % within q5childhome1 No children	2 100,0%	19 100,0%	21 100,0%

a. country = DE

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q5childhome1 No children Crosstabulation^a

			q5childhome1 No children		Total
			no	yes	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count % within q5childhome1 No children	1 50,0%	7 36,8%	8 38,1%
	partly agree	Count % within q5childhome1 No children	1 50,0%	10 52,6%	11 52,4%
	partly disagree	Count % within q5childhome1 No children	0 ,0%	2 10,5%	2 9,5%
Total		Count % within q5childhome1 No children	2 100,0%	19 100,0%	21 100,0%

a. country = DE

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count % within q5childhome1 No children	0 ,0%	2 10,5%	2 9,5%
	partly agree	Count % within q5childhome1 No children	0 ,0%	5 26,3%	5 23,8%
	partly disagree	Count % within q5childhome1 No children	2 100,0%	1 5,3%	3 14,3%
	completely disagree	Count % within q5childhome1 No children	0 ,0%	11 57,9%	11 52,4%
Total			2 100,0%	19 100,0%	21 100,0%

a. country = DE

q18general When security technology is available, we might just as well make use of it * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q18general When security technology is available, we might just as well make use of it	completely agree	Count % within q5childhome1 No children	0 ,0%	2 10,5%	2 9,5%
	partly agree	Count % within q5childhome1 No children	0 ,0%	7 36,8%	7 33,3%
	partly disagree	Count % within q5childhome1 No children	2 100,0%	3 15,8%	5 23,8%
	completely disagree	Count % within q5childhome1 No children	0 ,0%	7 36,8%	7 33,3%
Total			2 100,0%	19 100,0%	21 100,0%

a. country = DE

q19general Privacy should not be violated without reasonable suspicion of criminal intent *
q5childhome1 No children Crosstabulation^a

			q5childhome1 No children		Total
			no	yes	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count % within q5childhome1 No children	2 100,0%	13 68,4%	15 71,4%
	partly agree	Count % within q5childhome1 No children	0 ,0%	5 26,3%	5 23,8%
	neither agree nor disagree	Count % within q5childhome1 No children	0 ,0%	1 5,3%	1 4,8%
Total		Count % within q5childhome1 No children	2 100,0%	19 100,0%	21 100,0%

a. country = DE

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent *
q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count % within q5childhome1 No children	1 50,0%	12 63,2%	13 61,9%
	partly agree	Count % within q5childhome1 No children	1 50,0%	5 26,3%	6 28,6%
	partly disagree	Count % within q5childhome1 No children	0 ,0%	1 5,3%	1 4,8%
	completely disagree	Count % within q5childhome1 No children	0 ,0%	1 5,3%	1 4,8%
Total		Count % within q5childhome1 No children	2 100,0%	19 100,0%	21 100,0%

a. country = DE

q21general New security technologies are likely to be abused by governmental agencies * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count % within q5childhome1 No children	0 ,0%	5 26,3%	5 23,8%
	partly agree	Count % within q5childhome1 No children	0 ,0%	8 42,1%	8 38,1%
	neither agree nor disagree	Count % within q5childhome1 No children	2 100,0%	2 10,5%	4 19,0%
	partly disagree	Count % within q5childhome1 No children	0 ,0%	1 5,3%	1 4,8%
	completely disagree	Count % within q5childhome1 No children	0 ,0%	3 15,8%	3 14,3%
Total		Count % within q5childhome1 No children	2 100,0%	19 100,0%	21 100,0%

a. country = DE

q22general New security technologies are likely to be abused by criminals * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q22general New security technologies are likely to be abused by criminals	completely agree	Count % within q5childhome1 No children	0 ,0%	14 73,7%	14 66,7%
	partly agree	Count % within q5childhome1 No children	2 100,0%	5 26,3%	7 33,3%
Total		Count % within q5childhome1 No children	2 100,0%	19 100,0%	21 100,0%

a. country = DE

Crosstabs 2

country = DE

q24biom2 Airport * PlaneBinary Plane more than once a year / less Crosstabulation

			PlaneBinary Plane more than once a year / less		Total
			1-2 times a year or more	Less than 1 time a year	
q24biom2 Airport	no	Count	3	7	10
		% within PlaneBinary Plane more than once a year / less	33,3%	58,3%	47,6%
	yes	Count	6	5	11
		% within PlaneBinary Plane more than once a year / less	66,7%	41,7%	52,4%
Total		Count	9	12	21
		% within PlaneBinary Plane more than once a year / less	100,0%	100,0%	100,0%

a. country = DE

q56dilem1 Accept database and biometrics * PlaneBinary Plane more than once a year / less Crosstabulation

			PlaneBinary Plane more than once a year / less		Total
			1-2 times a year or more	Less than 1 time a year	
q56dilem1 Accept database and biometrics	no	Count	6	10	16
		% within PlaneBinary Plane more than once a year / less	66,7%	83,3%	76,2%
	yes	Count	3	2	5
		% within PlaneBinary Plane more than once a year / less	33,3%	16,7%	23,8%
Total		Count	9	12	21
		% within PlaneBinary Plane more than once a year / less	100,0%	100,0%	100,0%

a. country = DE

q24biom5 Central bus and train station * PublicBinary Public daily / less Crosstabulation^a

			PublicBinary Public daily / less		Total
			Less	Daily	
q24biom5 Central bus and train station	no	Count	13	3	16
		% within PublicBinary Public daily / less	72,2%	100,0%	76,2%
	yes	Count	5	0	5
		% within PublicBinary Public daily / less	27,8%	,0%	23,8%
Total		Count	18	3	21
		% within PublicBinary Public daily / less	100,0%	100,0%	100,0%

a. country = DE

q55dilem1 Accept registration of travel and fingerprints * PublicBinary Public daily / less Crosstabulation^a

			PublicBinary Public daily / less		Total
			Less	Daily	
q55dilem1 Accept registration of travel and fingerprints	no	Count	16	3	19
		% within PublicBinary Public daily / less	88,9%	100,0%	90,5%
	yes	Count	2	0	2
		% within PublicBinary Public daily / less	11,1%	,0%	9,5%
Total		Count	18	3	21
		% within PublicBinary Public daily / less	100,0%	100,0%	100,0%

a. country = DE

q35local1 Terrorists and criminals w court order * CarBinary Car daily / less Crosstabulation^a

			CarBinary Car daily / less		Total
			Less	Daily	
q35local1 Terrorists and criminals w court order	no	Count	2	1	3
		% within CarBinary Car daily / less	10,5%	50,0%	14,3%
	yes	Count	17	1	18
		% within CarBinary Car daily / less	89,5%	50,0%	85,7%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q35local2 Any w/o court order * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q35local2 Any w/o court order	no	Count	18	2	20
		% within CarBinary Car daily / less	94,7%	100,0%	95,2%
	yes	Count	1	0	1
		% within CarBinary Car daily / less	5,3%	,0%	4,8%
Total			19	2	21
			100,0%	100,0%	100,0%

a. country = DE

q35local3 Stolen vehicles * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q35local3 Stolen vehicles	no	Count	8	2	10
		% within CarBinary Car daily / less	42,1%	100,0%	47,6%
	yes	Count	11	0	11
		% within CarBinary Car daily / less	57,9%	,0%	52,4%
Total			19	2	21
			100,0%	100,0%	100,0%

a. country = DE

q35local4 Speeding * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q35local4 Speeding	no	Count	17	2	19
		% within CarBinary Car daily / less	89,5%	100,0%	90,5%
	yes	Count	2	0	2
		% within CarBinary Car daily / less	10,5%	,0%	9,5%
Total			19	2	21
			100,0%	100,0%	100,0%

a. country = DE

q35local5 Automatic accident reporting * CarBinary Car daily / less Crosstabulation

				CarBinary Car daily / less		Total
				Less	Daily	
q35local5 Automatic accident reporting	no	Count	6	1	7	
		% within CarBinary Car daily / less	31,6%	50,0%	33,3%	
	yes	Count	13	1	14	
		% within CarBinary Car daily / less	68,4%	50,0%	66,7%	
Total		Count	19	2	21	
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%	

a. country = DE

q36local Should eCall automatically be installed in all new cars? * CarBinary Car daily / less Crosstabulation^a

			CarBinary Car daily / less		Total
			Less	Daily	
q36local Should eCall automatically be installed in all new cars?	yes	Count	4	0	4
		% within CarBinary Car daily / less	21,1%	,0%	19,0%
	yes but possible to deactivate	Count	2	0	2
		% within CarBinary Car daily / less	10,5%	,0%	9,5%
	no, optional	Count	11	0	11
		% within CarBinary Car daily / less	57,9%	,0%	52,4%
	no, never	Count	2	2	4
		% within CarBinary Car daily / less	10,5%	100,0%	19,0%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q39local The possibility of locating all cars is privacy infringing * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q39local The possibility of locating all cars is privacy infringing	completely agree	Count	13	2	15
		% within CarBinary Car daily / less	68,4%	100,0%	71,4%
	partly agree	Count	4	0	4
		% within CarBinary Car daily / less	21,1%	,0%	19,0%
	completely disagree	Count	2	0	2
		% within CarBinary Car daily / less	10,5%	,0%	9,5%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q59dilem1 Accept locate car to prevent crime or terrorism * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q59dilem1 Accept locate car to prevent crime or terrorism	no	Count	11	2	13
		% within CarBinary Car daily / less	57,9%	100,0%	61,9%
	yes	Count	8	0	8
		% within CarBinary Car daily / less	42,1%	,0%	38,1%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q59dilem2 Accept speeding tickets * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q59dilem2 Accept speeding tickets	no	Count	17	2	19
		% within CarBinary Car daily / less	89,5%	100,0%	90,5%
	yes	Count	2	0	2
		% within CarBinary Car daily / less	10,5%	,0%	9,5%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q59dilem3 Accept register all movements * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q59dilem3 Accept register all movements	no	Count	18	2	20
		% within CarBinary Car daily / less	94,7%	100,0%	95,2%
	yes	Count	1	0	1
		% within CarBinary Car daily / less	5,3%	,0%	4,8%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q59dilem4 Accept only accidents * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q59dilem4 Accept only accidents	no	Count	9	0	9
		% within CarBinary Car daily / less	47,4%	,0%	42,9%
	yes	Count	10	2	12
		% within CarBinary Car daily / less	52,6%	100,0%	57,1%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q59dilem5 Accept only if voluntary * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q59dilem5 Accept only if voluntary	no	Count	6	0	6
		% within CarBinary Car daily / less	31,6%	,0%	28,6%
	yes	Count	13	2	15
		% within CarBinary Car daily / less	68,4%	100,0%	71,4%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q59dilem6 d.k. * CarBinary Car daily / less Crosstabulation

			CarBinary Car daily / less		Total
			Less	Daily	
q59dilem6 d.k.	no	Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%
Total		Count	19	2	21
		% within CarBinary Car daily / less	100,0%	100,0%	100,0%

a. country = DE

q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * PhoneBinary Phone daily / less Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count % within PhoneBinary Phone daily / less	1 6,7%	0 ,0%	1 4,8%
	partly agree	Count % within PhoneBinary Phone daily / less	3 20,0%	1 16,7%	4 19,0%
	neither agree nor disagree	Count % within PhoneBinary Phone daily / less	1 6,7%	1 16,7%	2 9,5%
	partly disagree	Count % within PhoneBinary Phone daily / less	2 13,3%	3 50,0%	5 23,8%
	completely disagree	Count % within PhoneBinary Phone daily / less	8 53,3%	1 16,7%	9 42,9%
Total			15 100,0%	6 100,0%	21 100,0%

a. country = DE

q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * EmailBinary Email daily / less Crosstabulation

			EmailBinary Email daily / less		Total
			Less	Daily	
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count % within EmailBinary Email daily / less	1 7,7%	0 ,0%	1 4,8%
	partly agree	Count % within EmailBinary Email daily / less	2 15,4%	2 25,0%	4 19,0%
	neither agree nor disagree	Count % within EmailBinary Email daily / less	2 15,4%	0 ,0%	2 9,5%
	partly disagree	Count % within EmailBinary Email daily / less	2 15,4%	3 37,5%	5 23,8%
	completely disagree	Count % within EmailBinary Email daily / less	6 46,2%	3 37,5%	9 42,9%
Total			13 100,0%	8 100,0%	21 100,0%

a. country = DE

q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * InternetBinary Internet daily / less Crosstabulation

			InternetBinary Internet daily / less		Total
			Less	Daily	
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count % within InternetBinary Internet daily / less	1 12,5%	0 ,0%	1 4,8%
	partly agree	Count % within InternetBinary Internet daily / less	1 12,5%	3 23,1%	4 19,0%
	neither agree nor disagree	Count % within InternetBinary Internet daily / less	2 25,0%	0 ,0%	2 9,5%
	partly disagree	Count % within InternetBinary Internet daily / less	2 25,0%	3 23,1%	5 23,8%
	completely disagree	Count % within InternetBinary Internet daily / less	2 25,0%	7 53,8%	9 42,9%
Total		Count % within InternetBinary Internet daily / less	8 100,0%	13 100,0%	21 100,0%

a. country = DE

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * PhoneBinary Phone daily / less Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count % within PhoneBinary Phone daily / less	11 73,3%	4 66,7%	15 71,4%
	partly agree	Count % within PhoneBinary Phone daily / less	2 13,3%	0 ,0%	2 9,5%
	partly disagree	Count % within PhoneBinary Phone daily / less	2 13,3%	2 33,3%	4 19,0%
Total		Count % within PhoneBinary Phone daily / less	15 100,0%	6 100,0%	21 100,0%

a. country = DE

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * EmailBinary Email daily / less Crosstabulation^a

			EmailBinary Email daily / less		Total
			Less	Daily	
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count % within EmailBinary Email daily / less	11 84,6%	4 50,0%	15 71,4%
	partly agree	Count % within EmailBinary Email daily / less	1 7,7%	1 12,5%	2 9,5%
	partly disagree	Count % within EmailBinary Email daily / less	1 7,7%	3 37,5%	4 19,0%
Total		Count % within EmailBinary Email daily / less	13 100,0%	8 100,0%	21 100,0%

a. country = DE

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * InternetBinary Internet daily / less Crosstabulation^a

			InternetBinary Internet daily / less		Total
			Less	Daily	
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count % within InternetBinary Internet daily / less	6 75,0%	9 69,2%	15 71,4%
	partly agree	Count % within InternetBinary Internet daily / less	1 12,5%	1 7,7%	2 9,5%
	partly disagree	Count % within InternetBinary Internet daily / less	1 12,5%	3 23,1%	4 19,0%
Total		Count % within InternetBinary Internet daily / less	8 100,0%	13 100,0%	21 100,0%

a. country = DE

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * PhoneBinary Phone daily / less Crosstabulation^a

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	14	3	17
		% within PhoneBinary Phone daily / less	93,3%	50,0%	81,0%
	partly agree	Count	0	2	2
		% within PhoneBinary Phone daily / less	,0%	33,3%	9,5%
	partly disagree	Count	1	1	2
		% within PhoneBinary Phone daily / less	6,7%	16,7%	9,5%
Total		Count	15	6	21
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = DE

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * EmailBinary Email daily / less Crosstabulation^a

			EmailBinary Email daily / less		Total
			Less	Daily	
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	11	6	17
		% within EmailBinary Email daily / less	84,6%	75,0%	81,0%
	partly agree	Count	2	0	2
		% within EmailBinary Email daily / less	15,4%	,0%	9,5%
	partly disagree	Count	0	2	2
		% within EmailBinary Email daily / less	,0%	25,0%	9,5%
Total	Count	13	8	21	
	% within EmailBinary Email daily / less	100,0%	100,0%	100,0%	

a. country = DE

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * InternetBinary Internet daily / less Crosstabulation^a

			InternetBinary Internet daily / less		Total
			Less	Daily	
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count % within InternetBinary Internet daily / less	6 75,0%	11 84,6%	17 81,0%
	partly agree	Count % within InternetBinary Internet daily / less			
	partly disagree	Count % within InternetBinary Internet daily / less			
Total		Count % within InternetBinary Internet daily / less			

a. country = DE

q47data Databases being used for something else than the original purpose is a serious privacy problem * PhoneBinary Phone daily / less Crosstabulation^a

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count % within PhoneBinary Phone daily / less	15 100,0%	5 83,3%	20 95,2%
	partly agree	Count % within PhoneBinary Phone daily / less	0 ,0%	1 16,7%	1 4,8%
Total		Count % within PhoneBinary Phone daily / less	15 100,0%	6 100,0%	21 100,0%

a. country = DE

q47data Databases being used for something else than the original purpose is a serious privacy problem^a
*** EmailBinary Email daily / less Crosstabulation**

			EmailBinary Email daily / less		Total
			Less	Daily	
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count % within EmailBinary Email daily / less	13 100,0%	7 87,5%	20 95,2%
	partly agree	Count % within EmailBinary Email daily / less	0 ,0%	1 12,5%	1 4,8%
Total		Count % within EmailBinary Email daily / less	13 100,0%	8 100,0%	21 100,0%

a. country = DE

q47data Databases being used for something else than the original purpose is a serious privacy problem^a
*** InternetBinary Internet daily / less Crosstabulation**

			InternetBinary Internet daily / less		Total
			Less	Daily	
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count % within InternetBinary Internet daily / less	8 100,0%	12 92,3%	20 95,2%
	partly agree	Count % within InternetBinary Internet daily / less	0 ,0%	1 7,7%	1 4,8%
Total		Count % within InternetBinary Internet daily / less	8 100,0%	13 100,0%	21 100,0%

a. country = DE

q51wire Eavesdropping is a serious violation of privacy * PhoneBinary Phone daily / less

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count % within PhoneBinary Phone daily / less	13 86,7%	4 66,7%	17 81,0%
	partly agree	Count % within PhoneBinary Phone daily / less	1 6,7%	2 33,3%	3 14,3%
	partly disagree	Count % within PhoneBinary Phone daily / less	1 6,7%	0 ,0%	1 4,8%
Total		Count % within PhoneBinary Phone daily / less	15 100,0%	6 100,0%	21 100,0%

a. country = DE

q51wire Eavesdropping is a serious violation of privacy * EmailBinary Email daily / less Crosstabulation

			EmailBinary Email daily / less		Total
			Less	Daily	
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count % within EmailBinary Email daily / less	10 76,9%	7 87,5%	17 81,0%
	partly agree	Count % within EmailBinary Email daily / less	3 23,1%	0 ,0%	3 14,3%
	partly disagree	Count % within EmailBinary Email daily / less	0 ,0%	1 12,5%	1 4,8%
Total		Count % within EmailBinary Email daily / less	13 100,0%	8 100,0%	21 100,0%

a. country = DE

q51wire Eavesdropping is a serious violation of privacy * InternetBinary Internet daily / less Crosstabulation

			InternetBinary Internet daily / less		Total
			Less	Daily	
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count % within InternetBinary Internet daily / less	6 75,0%	11 84,6%	17 81,0%
	partly agree	Count % within InternetBinary Internet daily / less	2 25,0%	1 7,7%	3 14,3%
	partly disagree	Count % within InternetBinary Internet daily / less	0 ,0%	1 7,7%	1 4,8%
Total		Count % within InternetBinary Internet daily / less	8 100,0%	13 100,0%	21 100,0%

a. country = DE

**q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy *
PhoneBinary Phone daily / less Crosstabulation**

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count % within PhoneBinary Phone daily / less	9 60,0%	2 33,3%	11 52,4%
	partly agree	Count % within PhoneBinary Phone daily / less	3 20,0%	2 33,3%	5 23,8%
	neither agree nor disagree	Count % within PhoneBinary Phone daily / less	2 13,3%	0 ,0%	2 9,5%
	partly disagree	Count % within PhoneBinary Phone daily / less	1 6,7%	0 ,0%	1 4,8%
	completely disagree	Count % within PhoneBinary Phone daily / less	0 ,0%	2 33,3%	2 9,5%
Total		Count % within PhoneBinary Phone daily / less	15 100,0%	6 100,0%	21 100,0%

a. country = DE

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy *
EmailBinary Email daily / less Crosstabulation

			EmailBinary Email daily / less		Total
			Less	Daily	
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count % within EmailBinary Email daily / less	7 53,8%	4 50,0%	11 52,4%
	partly agree	Count % within EmailBinary Email daily / less	5 38,5%	0 ,0%	5 23,8%
	neither agree nor disagree	Count % within EmailBinary Email daily / less	1 7,7%	1 12,5%	2 9,5%
	partly disagree	Count % within EmailBinary Email daily / less	0 ,0%	1 12,5%	1 4,8%
	completely disagree	Count % within EmailBinary Email daily / less	0 ,0%	2 25,0%	2 9,5%
Total		Count % within EmailBinary Email daily / less	13 100,0%	8 100,0%	21 100,0%

a. country = DE

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy *
InternetBinary Internet daily / less Crosstabulation

			InternetBinary Internet daily / less		Total
			Less	Daily	
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count % within InternetBinary Internet daily / less	3 37,5%	8 61,5%	11 52,4%
	partly agree	Count % within InternetBinary Internet daily / less	4 50,0%	1 7,7%	5 23,8%
	neither agree nor disagree	Count % within InternetBinary Internet daily / less	1 12,5%	1 7,7%	2 9,5%
	partly disagree	Count % within InternetBinary Internet daily / less	0 ,0%	1 7,7%	1 4,8%
	completely disagree	Count % within InternetBinary Internet daily / less	0 ,0%	2 15,4%	2 9,5%
Total		Count % within InternetBinary Internet daily / less	8 100,0%	13 100,0%	21 100,0%

a. country = DE

q58dilem1 Accept all access for counter terrorism^a * PhoneBinary Phone daily / less
Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q58dilem1 Accept all access for counter terrorism	no	Count	14	5	19
		% within PhoneBinary Phone daily / less	93,3%	83,3%	90,5%
	yes	Count	1	1	2
		% within PhoneBinary Phone daily / less	6,7%	16,7%	9,5%
Total		Count	15	6	21
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = DE

q58dilem1 Accept all access for counter terrorism^a * EmailBinary Email daily / less
Crosstabulation

			EmailBinary Email daily / less		Total
			Less	Daily	
q58dilem1 Accept all access for counter terrorism	no	Count	12	7	19
		% within EmailBinary Email daily / less	92,3%	87,5%	90,5%
	yes	Count	1	1	2
		% within EmailBinary Email daily / less	7,7%	12,5%	9,5%
Total		Count	13	8	21
		% within EmailBinary Email daily / less	100,0%	100,0%	100,0%

a. country = DE

q58dilem1 Accept all access for counter terrorism * InternetBinary Internet daily / less
Crosstabulation

			InternetBinary Internet daily / less		Total
			Less	Daily	
q58dilem1 Accept all access for counter terrorism	no	Count	7	12	19
		% within InternetBinary Internet daily / less	87,5%	92,3%	90,5%
	yes	Count	1	1	2
		% within InternetBinary Internet daily / less	12,5%	7,7%	9,5%
Total			8	13	21
			100,0%	100,0%	100,0%

a. country = DE

q34local1 Terrorists and criminals w court order * PhoneBinary Phone daily / less
Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q34local1 Terrorists and criminals w court order	no	Count	2	1	3
		% within PhoneBinary Phone daily / less	13,3%	16,7%	14,3%
	yes	Count	13	5	18
		% within PhoneBinary Phone daily / less	86,7%	83,3%	85,7%
Total			15	6	21
			100,0%	100,0%	100,0%

a. country = DE

q34local2 Any w/o court order * PhoneBinary Phone daily / less Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q34local2 Any w/o court order	no	Count	15	5	20
		% within PhoneBinary Phone daily / less	100,0%	83,3%	95,2%
	yes	Count	0	1	1
		% within PhoneBinary Phone daily / less	,0%	16,7%	4,8%
Total		Count	15	6	21
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = DE

q34local3 Emergency * PhoneBinary Phone daily / less Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q34local3 Emergency	no	Count	1	1	2
		% within PhoneBinary Phone daily / less	6,7%	16,7%	9,5%
	yes	Count	14	5	19
		% within PhoneBinary Phone daily / less	93,3%	83,3%	90,5%
Total		Count	15	6	21
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = DE

q34local4 Never * PhoneBinary Phone daily / less Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q34local4 Never	no	Count	14	6	20
		% within PhoneBinary Phone daily / less	93,3%	100,0%	95,2%
	yes	Count	1	0	1
		% within PhoneBinary Phone daily / less	6,7%	,0%	4,8%
Total		Count	15	6	21
		% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%

a. country = DE

q34local5 d.k. * PhoneBinary Phone daily / less Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q34local5 d.k. no	Count	15	6	21	
	% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%	
Total	Count	15	6	21	
	% within PhoneBinary Phone daily / less	100,0%	100,0%	100,0%	

a. country = DE

q52protect1 Anonymous calling cards * PhoneBinary Phone daily / less Crosstabulation

				PhoneBinary Phone daily / less		Total
				Less	Daily	
q52protect1 Anonymous calling cards	no	Count		5	3	8
		% within PhoneBinary Phone daily / less		33,3%	50,0%	38,1%
	yes	Count		10	3	13
		% within PhoneBinary Phone daily / less		66,7%	50,0%	61,9%
Total		Count		15	6	21
		% within PhoneBinary Phone daily / less		100,0%	100,0%	100,0%

a. country = DE

q37local The possibility of locating all mobile phones is privacy infringing * PhoneBinary Phone daily / less Crosstabulation

			PhoneBinary Phone daily / less		Total
			Less	Daily	
q37local The possibility of locating all mobile phones is privacy infringing	completely agree	Count % within PhoneBinary Phone daily / less	10 66,7%	4 66,7%	14 66,7%
	partly agree	Count % within PhoneBinary Phone daily / less	3 20,0%	1 16,7%	4 19,0%
	neither agree nor disagree	Count % within PhoneBinary Phone daily / less	1 6,7%	0 ,0%	1 4,8%
	completely disagree	Count % within PhoneBinary Phone daily / less	1 6,7%	1 16,7%	2 9,5%
Total		Count % within PhoneBinary Phone daily / less	15 100,0%	6 100,0%	21 100,0%

a. country = DE

q52protect2 Encryption programmes * EmailBinary Email daily / less Crosstabulation

			EmailBinary Email daily / less		Total
			Less	Daily	
q52protect2 Encryption programmes	no	Count % within EmailBinary Email daily / less	2 15,4%	4 50,0%	6 28,6%
	yes	Count % within EmailBinary Email daily / less	11 84,6%	4 50,0%	15 71,4%
Total		Count % within EmailBinary Email daily / less	13 100,0%	8 100,0%	21 100,0%

a. country = DE

q52protect3 Identity management * InternetBinary Internet daily / less Crosstabulation

				InternetBinary Internet daily / less		Total
				Less	Daily	
q52protect3 Identity management	no	Count	2	6	8	
		% within InternetBinary Internet daily / less	25,0%	46,2%	38,1%	
	yes	Count	6	7	13	
		% within InternetBinary Internet daily / less	75,0%	53,8%	61,9%	
Total		Count	8	13	21	
		% within InternetBinary Internet daily / less	100,0%	100,0%	100,0%	

a. country = DE

*****bonus crosstabs – public weekly & car weekly*******Crosstabs****q24biom5 Central bus and train station * PublicBinary2 Public weekly / less Crosstabulation**

				PublicBinary2 Public weekly / less		Total
				less than once a week	at least once a week	
q24biom5 Central bus and train station	no	Count	11	5	16	
		% within PublicBinary2 Public weekly / less	73,3%	83,3%	76,2%	
	yes	Count	4	1	5	
		% within PublicBinary2 Public weekly / less	26,7%	16,7%	23,8%	
Total		Count	15	6	21	
		% within PublicBinary2 Public weekly / less	100,0%	100,0%	100,0%	

q35local1 Terrorists and criminals w court order * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q35local1 Terrorists and criminals w court order	no	Count	2	1	3
		% within CarBinary2 Car weekly / less	14,3%	14,3%	14,3%
	yes	Count	12	6	18
		% within CarBinary2 Car weekly / less	85,7%	85,7%	85,7%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

q35local2 Any w/o court order * CarBinary2 Car weekly / less Crosstabulation

				CarBinary2 Car weekly / less		Total
				less than once a week	at least once a week	
q35local2 Any w/o court order	no	Count	13	7	20	
		% within CarBinary2 Car weekly / less	92,9%	100,0%	95,2%	
	yes	Count	1	0	1	
		% within CarBinary2 Car weekly / less	7,1%	,0%	4,8%	
Total		Count	14	7	21	
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%	

q35local3 Stolen vehicles * CarBinary2 Car weekly / less Crosstabulation

				CarBinary2 Car weekly / less		Total
				less than once a week	at least once a week	
q35local3 Stolen vehicles	no	Count	6	4	10	
		% within CarBinary2 Car weekly / less	42,9%	57,1%	47,6%	
	yes	Count	8	3	11	
		% within CarBinary2 Car weekly / less	57,1%	42,9%	52,4%	
Total		Count	14	7	21	
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%	

q35local4 Speeding * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q35local4 Speeding	no	Count	12	7	19
		% within CarBinary2 Car weekly / less	85,7%	100,0%	90,5%
	yes	Count	2	0	2
		% within CarBinary2 Car weekly / less	14,3%	,0%	9,5%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

q35local5 Automatic accident reporting * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q35local5 Automatic accident reporting	no	Count	4	3	7
		% within CarBinary2 Car weekly / less	28,6%	42,9%	33,3%
	yes	Count	10	4	14
		% within CarBinary2 Car weekly / less	71,4%	57,1%	66,7%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

q36local Should eCall automatically be installed in all new cars? * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q36local Should eCall automatically be installed in all new cars?	yes	Count % within CarBinary2 Car weekly / less	3 21,4%	1 14,3%	4 19,0%
	yes but possible to deactivate	Count % within CarBinary2 Car weekly / less	2 14,3%	0 ,0%	2 9,5%
	no, optional	Count % within CarBinary2 Car weekly / less	8 57,1%	3 42,9%	11 52,4%
	no, never	Count % within CarBinary2 Car weekly / less	1 7,1%	3 42,9%	4 19,0%
Total			14 100,0%	7 100,0%	21 100,0%

q39local The possibility of locating all cars is privacy infringing * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q39local The possibility of locating all cars is privacy infringing	completely agree	Count % within CarBinary2 Car weekly / less	8 57,1%	7 100,0%	15 71,4%
	partly agree	Count % within CarBinary2 Car weekly / less	4 28,6%	0 ,0%	4 19,0%
	completely disagree	Count % within CarBinary2 Car weekly / less	2 14,3%	0 ,0%	2 9,5%
Total			14 100,0%	7 100,0%	21 100,0%

q59dilem1 Accept locate car to prevent crime or terrorism * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q59dilem1 Accept locate car to prevent crime or terrorism	no	Count	8	5	13
		% within CarBinary2 Car weekly / less	57,1%	71,4%	61,9%
	yes	Count	6	2	8
		% within CarBinary2 Car weekly / less	42,9%	28,6%	38,1%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

q59dilem2 Accept speeding tickets * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q59dilem2 Accept speeding tickets	no	Count	12	7	19
		% within CarBinary2 Car weekly / less	85,7%	100,0%	90,5%
	yes	Count	2	0	2
		% within CarBinary2 Car weekly / less	14,3%	,0%	9,5%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

q59dilem3 Accept register all movements * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q59dilem3 Accept register all movements	no	Count	13	7	20
		% within CarBinary2 Car weekly / less	92,9%	100,0%	95,2%
	yes	Count	1	0	1
		% within CarBinary2 Car weekly / less	7,1%	,0%	4,8%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

q59dilem4 Accept only accidents * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q59dilem4 Accept only accidents	no	Count	7	2	9
		% within CarBinary2 Car weekly / less	50,0%	28,6%	42,9%
	yes	Count	7	5	12
		% within CarBinary2 Car weekly / less	50,0%	71,4%	57,1%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

q59dilem5 Accept only if voluntary * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q59dilem5 Accept only if voluntary	no	Count	6	0	6
		% within CarBinary2 Car weekly / less	42,9%	,0%	28,6%
	yes	Count	8	7	15
		% within CarBinary2 Car weekly / less	57,1%	100,0%	71,4%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

q59dilem6 d.k. * CarBinary2 Car weekly / less Crosstabulation

			CarBinary2 Car weekly / less		Total
			less than once a week	at least once a week	
q59dilem6 d.k.	no	Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%
Total		Count	14	7	21
		% within CarBinary2 Car weekly / less	100,0%	100,0%	100,0%

Annex 7 - Comments from the questionnaire

- Sicherheitstechnologien sind nicht nur Internet, Scanner, Video
- Neue Sicherheitstechnologien entwickeln, Terrorismus keinen technologischen Vorsprung lassen
- Fragen stark staatslastig
- Kriminalisierung der Bürger
- Technikentwicklung nicht um jeden Preis, Gesellschaft nicht aus den Augen verlieren, Kriminalitätsursachen bekämpfen
- Einige Antwortmöglichkeiten zu unscharf
- Fehleranfälligkeit von Computersystemen bei Zusammenführung großer Datenmengen berücksichtigen
- Videoaufzeichnungen akzeptabel wenn DS beachtet wird
- Sicherheitstechnologie im Notfall nutzen, Angst vor Missbrauch
- Sicherheitstechnologie macht Debatte nach Frieden teilweise sinnlos
- Sicherheitstechnologien werden immer missbraucht werden können